UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

VoIP Network Analyzer

Trabajo Final de Grado

Presentado a la facultad

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona (ETSETB)

Universitat Politècnica de Catalunya

Realizado por

Anna Martínez Querol

Como cumplimiento parcial de los requisitos para obtener el grado en

Sistemas de Telecomunicación

Director: Jaume Xarrié Sánchez

Codirector: Oscar Esparza Martín

Barcelona, Septiembre 2016

Abstract

Globalization and technological growth are highly linked to the rise of ICT (Information and Communications Technology) and therefore to computer and communications services, but the boom doesn't imply that the services offered by providers of Internet and the quality that the customers perceive are in the same proportions.

Therefore, this work is aimed at developing a model audit using tools and methods to evaluate different measuring parameters of the quality of service from Voice over IP. The result of this work is a document that analyzes the technological infrastructure and the parameters of quality measurement network, which will determine if a customer can receive these services with the highest quality.

.

Resum

La globalització i el creixement tecnològic estan inexorablement lligats a l'apogeu de les TIC (Tecnologies de la Informació i Comunicació) i per tant als serveis informàtics i a les comunicacions, però aquest apogeu no implica que els serveis oferts pels proveïdors de serveis d'Internet als clients i la seva qualitat creixin de la mateixa manera.

Per això, aquest treball està enfocat a desenvolupar un model d'auditoria utilitzant eines i mètodes per avaluar els diferents paràmetres de mesura de la qualitat del servei de Veu sobre IP. El resultat d'aquest treball és un document que analitza la infraestructura tecnològica i en el qual es detallen els paràmetres de mesura de qualitat de la xarxa, que determinaran si un client pot rebre aquests serveis amb la màxima qualitat.

Resumen

La globalización y el crecimiento tecnológico están inexorablemente ligados al auge de las TIC (Tecnologías de la Información y Comunicación) y por ende a los servicios informáticos y de comunicaciones, pero ese auge no implica que los servicios ofrecidos por los proveedores de servicios de Internet a los clientes y su calidad crezcan en las mismas proporciones.

Por ello, este trabajo está dirigido a desarrollar un modelo de auditoría utilizando herramientas y métodos para evaluar los diferentes parámetros de medida de la calidad del servicio de Voz sobre IP. El resultado de este trabajo es un documento que analiza la infraestructura tecnológica y en el que se detallan los parámetros de medida de calidad de la red, que determinarán si un cliente puede recibir dichos servicios con la máxima calidad.

Agradecimientos

A todos mis profesores por haber sido parte fundamental durante mi formación académica, pero en especial a Oscar Esparza, codirector de este trabajo, por haber tenido la paciencia, la dedicación y la confianza para apoyarme en la realización de este trabajo, gracias.

De la misma manera agradezco a Tpartner, y en especial a Jaume Xarrié la oportunidad de poder realizar este trabajo con ellos.

Por último y no menos importante, a mis padres, Juan Carlos y Fina, y a mis hermanos Carlos y Víctor, que han estado incondicionalmente a mi lado en este proyecto y en los que me quedan aún por realizar, gracias, sin vosotros, vuestro ánimo y vuestra manera de enseñarme y educarme no hubiese podido concluir el trabajo.

Tampoco puedo olvidar a todos estos amigos que han estado apoyándome día a día des del momento en que inicié la carrera, hasta día de hoy, amigos de siempre, de la universidad y amigos que me han demostrado que son más que amigos, y han estado a mi lado cuando todo parecía que no saldría adelante, gracias por confiar siempre en mi: Lana, Azra, Àlex, Íngrid, Laura, Chantal, David, Dèlia, Gabriela, Cristina, Juanito, Marc, Jordi, Pablo, Marc, Ferran, Anna, Cristina, Aleix, Arnau, Jazmín, Lorena, Marta…y a toda mi familia de Telecogresca. No tengo palabras para expresar por todo lo que os estoy agradecida así que solo puedo decir, gracias de corazón a todos.

Histórico de revisiones y registro de aprobación

Revisión	Fecha	Finalidad
0	13/05/2016	Creación del documento
1	30/05/2016	Revisión del documento
2	12/07/2016	Revisión del documento
3	1/09/2016	Revisión del documento

LISTA DE DISTRIBUCIÓN

Nombre	Mail
Anna Martínez Querol	annamtnezquerol@gmail.com
Jaume Xarrié Sánchez	jaume.xarrie@tpartner.net
Óscar Esparza Martín	oesparza@entel.upc.edu

Escrito por:		Revisado y aprobado por	
Fecha	16/05/2016	Fecha	1/05/2016
Nombre	Anna Martínez Querol	Nombre	Jame Xarrié Sánchez
Posición	Autora del proyecto	Posición	Supervisor del proyecto

Índice

Lista de Figuras

Lista de tablas:

1. Introducción

Una de las necesidades básicas del ser humano, es la de comunicarse. La tecnología crece y evoluciona, acorta distancias y nos mantiene siempre en contacto. Las redes IP, los servicios y las aplicaciones telemáticas que se desarrollan sobre ellas han experimentado un auge extraordinario.

Entre estas nuevas aplicaciones destacan: la voz sobre IP[1], la videoconferencia y las video llamadas.

Para poder utilizar este tipo de aplicaciones, que incluyen video y audio, la red sobre la que se desarrolla debe garantizar un mínimo de calidad de servicio para su correcto funcionamiento.

Los usuarios se han acostumbrados a un alto nivel de calidad en los servicios de telefonía y televisión, lo que implica la exigencia de ese mismo nivel de calidad a las redes privadas y accesos a Internet.

Con independencia de que el nuevo modelo de redes esté presente en todas las sociedades, de que la capacidad de las redes está siendo desaprovechada, de la gran versatilidad y de los bajos costes que supone ésta tecnología, se debe estudiar y analizar ésta tecnología para conocer sus ventajas e inconvenientes. Debemos intentar proporcionar al usuario final de la red las mejores prestaciones, para poder garantizar esa calidad. Por eso, cada vez más, los usuarios finales, las operadoras, los administradores de redes privadas y los desarrolladores de aplicaciones demandan auditorias de Calidad de Servicio.[2] Este proyecto se centrará en esa demanda de Auditorias de Calidad y de Servicio.

1.1. Motivaciones

Tpartner Network Service S.L, es una empresa catalana integradora de soluciones tecnológicas y especializadas en la comunicación y seguridad para PYMES. Es Business Partner de grandes empresas como Alcatel-Lucent, Siemens-Unify y Cisco System entre otras.

Los ejes que vertebran la diferenciación de Tpartner frente a sus competidores son: la alta cualificación de su equipo, su compromiso con la innovación y su management.

El rápido desarrollo de la tecnología VoIP ha comportado una serie de problemas ligados a la seguridad de ésta tecnología y la calidad del servicio que recibe el usuario, entender soluciona estos problemas ha servido de incentivo para el desarrollo de este proyecto.

Como ya he señalado, cuando el cliente decide utilizar esta tecnología y contratar un proveedor de servicios de VoIP, espera recibir un mínimo de calidad en el servicio que contrata. Si no está satisfecho, exige a su proveedor de VoIP una solución satisfactoria. Pero el cliente no sabe que ésta tecnología tiene una serie de limitaciones y que muchas veces no dependen del proveedor si no del propio cliente, que interfiere en el buen funcionamiento de la VoIP.

[1] De ahora en adelante llamaremos a la voz sobre IP, VoIP en inglés Voice over Internet Protocol.
[2] QoS en inglés Quality of Service, QoS

Para garantizar esos mínimos de calidad se tomarán una serie de medidas y se estudiarán una serie de herramientas que nos permitirán generar un informe que se le entregará al cliente, en el que se determine si es apto o no para que la VoIP funcione satisfactoriamente.

1.2. Objetivos del proyecto

1. Decidir y ejecutar un sistema de adquisición de datos para poder determinar si la red del cliente cumple los mínimos de calidad para garantizar que la VoIP funcionará correctamente.
2. Desarrollar un informe que se le entregará al cliente, por si después de la instalación de la VoIP el cliente exige responsabilidades por su incorrecto funcionamiento, lo que permitirá eximir de responsabilidad al proveedor.

Para llevar a cabo este proyecto se desarrollarán dos fases:

- En la primera se informará al cliente sobre las ventajas y limitaciones de la VoIP, y se realizará una auditoria previa a su instalación, estudiando la red del cliente, los servicios contratados y comprobando si los sistemas de los que dispone son aptos y cumplen unos requisitos mínimos para poder realizar el despliegue con garantías
- Una vez hecho el test de calidad y seguridad, que determina si el cliente es apto para poder utilizar VoIP, en una segunda fase se le instalará y se desplegarán una serie de herramientas que nos permitirán supervisar regularmente la red del cliente, para evaluar una serie de parámetros clave, que, si se desvían de los estándares, podrán ayudarnos a prevenir y resolver una avería de forma eficaz. Aplicaremos la filosofía “win to win” proporcionando beneficios para el cliente (máxima calidad) y beneficios para la empresa (disponer de una prueba física que nos permita derivar la solución al proveedor).

El resultado de la implementación de esta última fase conseguirá que se minimicen los problemas tanto los del usuario como los de la empresa que le ofrece el servicio y portando la mejora de la QoS (Calidad del Servicio) y la del QoE (Calidad de Experiencia).

1.3. Metodología

La metodología implementada en el desarrollo de la investigación consta de tres etapas:

1. Revisión de la literatura y estudio previo:

   Es necesario un estudio y compresión de las redes de Voz sobre IP, desde su funcionamiento dentro de las redes de datos, los problemas que presenta, las arquitecturas más comunes usadas, los protocolos implementados, la seguridad de esta tecnología…etc. Además de comprender como funciona la VoIP, se han tenido que evaluar las ventajas y desventajas de esta tecnología.

   Se han estudiado los parámetros que afectan la calidad de servicio en telefonía IP y los estándares que debe cumplir cada parámetro para garantizar que una llamada Voz sobre IP se establezca y desarrolle con calidad.

2. Pruebas:

   Se estudiarán una serie de herramientas para poder realizar la auditoría sobre la calidad del servicio, y así poder realizar un informe.

3. Conclusiones y resultados:

   A partir del informe generado, se elabora una serie de conclusiones determinando si la red del cliente es apta o no apta para esta tecnología y se proponen una serie de recomendaciones para mejorar su red.

1.4. Estructura de la memoria

La memoria se ha dividido 4 capítulos.

El primer bloque es teórico, y después del capítulo inicial de introducción, donde se intenta que el lector se familiarice con el contexto del proyecto las motivaciones y objetivos se intentan cumplir. En los dos capítulos siguientes se explica la tecnología de voz sobre IP, para poder entender los problemas que derivan de ésta y también se trata la calidad del servicio y qué parámetros son importantes para que se puedan medir y analizar y por tanto conocer si un sistema es apto o no apto para que la VoIP tenga un mínimo de calidad.

El segundo bloque es práctico, y en él se explica qué herramienta se ha utilizado, cómo funciona y como nos permitirá medir los parámetros de calidad que nos ayudarán a generar el informe final que se le entregará al cliente.

Por último, las conclusiones y anexos.

2. Introducción a la voz sobre IP

La "Voz sobre Protocolo de Internet", conocida como Voz IP, es una tecnología que nos permite usar el protocolo de Internet[3] para encapsular la voz en paquetes para posteriormente ser transmitida mediante una red de datos de forma digital, que a diferencia de las redes de telefonía convencionales PSTN[4], lo hacen de forma analógica.

En sus orígenes, el protocolo de Internet, fue desarrollado para redes de transmisión de datos, pero debido a sus diferentes aplicaciones y éxito, ha permitido establecer otro tipo de comunicaciones como, voz, vídeo e imágenes.

Para poder comprender la tecnología VoIP y evaluar sus ventajas y desventajas, es necesario entender varios conceptos para ser capaces de evaluar esta tecnología.[5]

Conceptos:

- *Voz sobre IP (VoIP)*, es la tecnología (conjunto de normas, dispositivos y protocolos), que utiliza el protocolo IP para transmitir la voz y llegar a su destino.
- *Telefonía sobre IP*, es el servicio telefónico de venta al público, la numeración física, realizado con tecnología de VoIP.
- *Protocolo de red IP*, es el sistema de reglas que divide sus paquetes IP en una cabecera, para el control de la comunicación y una carga útil o payload de transporte de datos.

2.1. Red de Telefonía Pública Conmutada: PSTN

La Red PSTN, se encarga de enlazar los terminales a través de la conmutación de circuitos físicos durante un tiempo predeterminado entre emisor y receptor.

2.1.1. Proceso de una llamada telefónica convencional

Figura 2:1 Proceso de una llamada telefónica convencional

[3] IP- Internet Protocol, mirar glosario para más siglas
[4] PSTN- Public Switched Telephone Network, red de telefonía pública conmutada.
[5] En este proyecto no se han tenido en cuenta aspectos de seguridad, vulnerabilidades y amenazas ya que es un tema tan extenso que merecería un trabajo a parte.

2.1.1.1. La experiencia del usuario

1. Descolgar el teléfono físico y al oír el tono, nos indica que ya tenemos conexión con el proveedor para marcar el número telefónico del receptor.
2. Marcamos el número telefónico del receptor.
3. El teléfono del receptor suena y si descuelga el teléfono se inicia la comunicación.

2.1.1.2. La realidad de la comunicación:

1. Al descolgar el teléfono para marcar el número telefónico, se hace una conexión en forma analógica con la central telefónica, (exactamente con la placa de abonado que controla nuestra línea).
2. La placa de abonado realiza la conversión analógica – digital y la señal se convierte a un PCM de 64 kbps (señal sin pérdida de información y compresión).
3. La llamada se transmite por el conmutador del operador hasta su destino, creando una conexión entre el emisor y el receptor.
4. El operador enlaza varios conmutadores para lograr la llamada.
5. La placa de abonado decodifica los tonos de discado (DTMF).
6. El teléfono del receptor suena y contesta la llamada, la conexión abre el circuito, se comunican las dos partes y finalizan la llamada. Al colgar el teléfono el circuito se cierra y automáticamente libera las líneas que participaron en la comunicación.

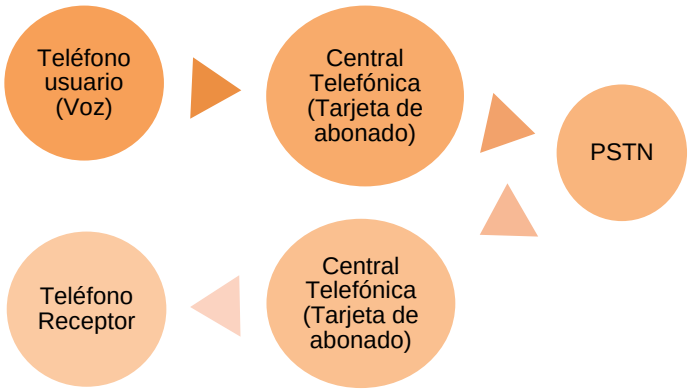


Figura 2:2 Proceso de una llamada convencional.

2.1.2. Componentes que intervienen en una llamada sobe una red telefónica convencional

- Codificadores de voz.
- Decodificadores de voz.
- Teléfonos.
- Switches.
- Central telefónica[6].

[6] Conocida también como PBX, en inglés Public Branch Exchange.

2.1.3. Características de una red PSTN

- Dedica un circuito a la llamada hasta que finaliza sin importar que los usuarios estén hablando o en silencio.
- Ofrece a cada usuario un circuito para señales analógicas con una banda base de 4KHz para cada conversación entre dos personas.
- El coste para el usuario por la ocupación del circuito depende de la distancia entre los extremos y la duración de la conexión
- Consta de Medios de transmisión y centrales de conmutación.
- Esta tecnología se divide por un tiempo fijo, una vez establecida la comunicación se garantiza el ancho de banda necesario para poder hablar sin interrupciones.

2.2. Red voz sobre IP

La telefonía IP, envía varias conversaciones a través de un mismo medio virtual, donde se comprimen y descomprimen de la manera más eficiente los paquetes, que se encapsulan y circulan por cualquier red IP, incluyendo aquellas conectadas a Internet. Para la comunicación por VoIP, tanto el emisor como el receptor deben tener un servicio VoIP.

Figura 2:3 Esquema de telefonía de red sobre IP

Para que dos terminales IP puedan comunicarse, es necesaria una señalización que se realiza mediante diferentes protocolos, el más utilizado es el SIP[7], pero el protocolo que se encarga del transporte de voz es el RTP[8].

2.2.1. Proceso de una llamada de telefonía IP[9]

1. Cuando el usuario levanta el auricular para realizar la llamada, se envía automáticamente una señal al ATA[10].
2. El ATA la recibe y envía un tono de llamada, con esto se encuentra conectado Internet.
3. Se marca el número del receptor, mediante un conversor los números se digitalizan y son almacenados por un periodo de tiempo.
4. Los datos del número telefónico son enviados al proveedor de VoIP.
5. Los servidores del proveedor VoIP validan el número especificado por el emisor.
6. Los servidores determinan a quien corresponde el número marcado y lo convierten a una dirección IP.

[7] SIP- Sesion Initation Protocol
[8] RTP – Real Time Protocol
[9] Para este ejemplo, se manejan teléfonos conectados a un adaptador de teléfono analógico, que se encarga de la conversión de las señales analógicas a digital y viceversa.
[10] ATA – Adaptador de Teléfono Analógico

7. El proveedor conecta los dos equipos que están realizando la llamada. En el extremo del receptor, ocurre el mismo procedimiento, pero, al contrario, la señal es enviada al ATA y éste se encarga de convertirla a analógica, la cual hace que el teléfono suene.
8. Una vez que el receptor levanta el auricular del teléfono, se establece una comunicación entre los servidores donde cada sistema espera recibir paquetes RTP[11], con los paquetes de datos de voz del otro.
9. Cuando finaliza la llamada el teléfono se cuelga y el circuito que estaba previamente establecido es cerrado.
10. El ATA del receptor o el emisor según el que haya colgado envía una señal al proveedor VoIP que le comunica que la llamada ha finalizado.

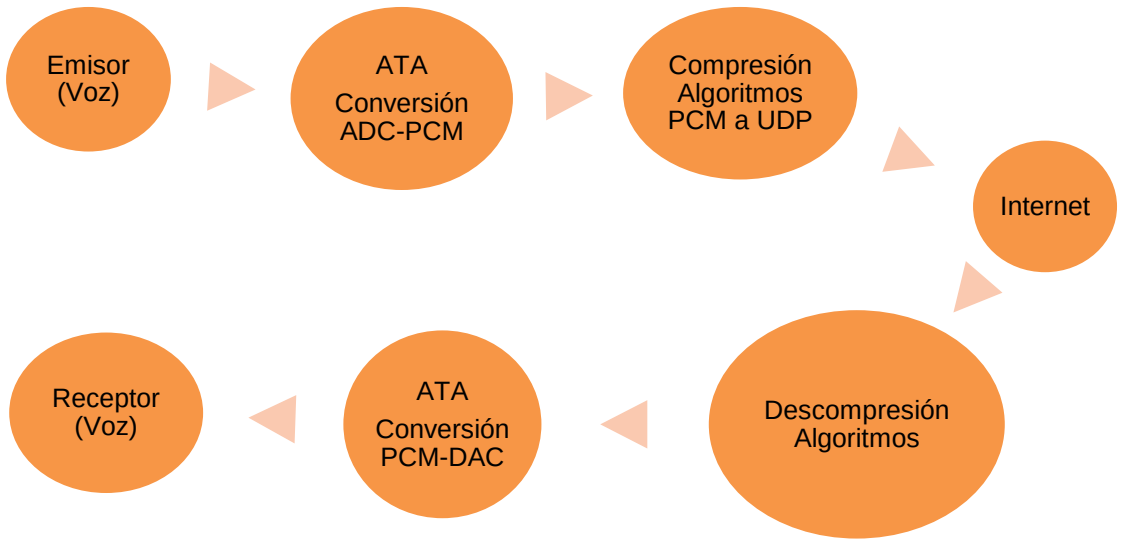


Figura 2:4 Proceso de una llamada de telefonía IP.

¿Cómo funciona realmente?

Como ya hemos mencionado, la VoIP funciona mediante la digitalización de la voz en paquetes de datos para su envío y su posterior conversión en voz en el destino.

Podemos ver en la figura 4 que la voz es convertida en paquetes de datos mediante un conversor ADC[12] y se transmite al destino mediante el protocolo RTP[13] donde se transforma otra vez en formato analógico con el conversor DAC[14].

La utilización del codificador y decodificador es importante para el rendimiento de la red y su velocidad de comunicación y los protocolos de señalización también lo son porqué se encargan de controlar la sesión: establecimiento, inicio, modificación y terminación de la llamada entre los usuarios.

[11] RTP – Real-time Transport Protocol.
[12] ADC- Analog to digital Converter.
[13] RTP - Real-time Transport Protocol.
[14] DAC – Digital to Analog Converter.

2.2.2. Servicios y equipos de voz necesarios para la tecnología VoIP

- Tener contratada una conexión a Internet de banda ancha.
- Teléfono tradicional con un adaptador o bien un teléfono habilitado para voz sobre IP o software de voz sobre IP en el ordenador.

2.2.3. Componentes principales de VoIP

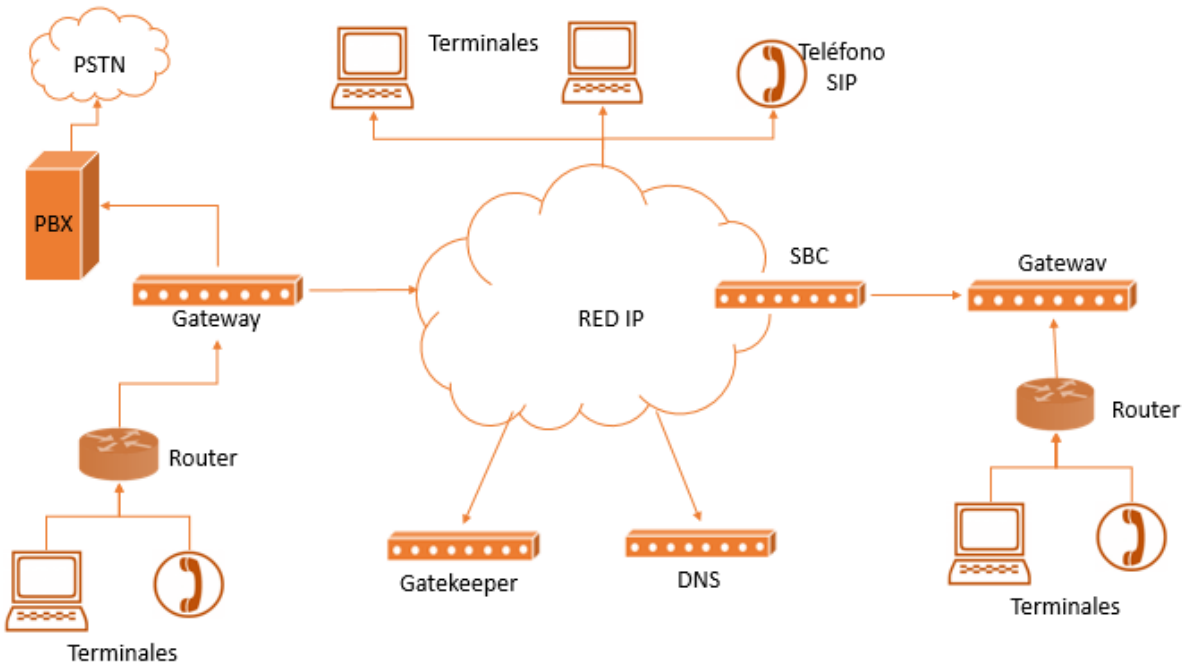


Figura 2:5 Elementos de una red VoIP

2.2.3.1. El usuario

Es quien origina y recibe las llamadas de voz

2.2.3.2. Los terminales

Son teléfonos VoIP, vienen a ser los sustitutos de los teléfonos. Pueden estar basados en hardware (como los teléfonos tradicionales) o en software (softphone, que pueden estar en un ordenador personal, una PDA o un teléfono móvil).

2.2.3.3. Los servidores

Son los equipos que realizan las operaciones de base de datos en tiempo real: contabilidad, recolección de datos, enrutamiento, administración y control del servicio. Normalmente en los servidores se instala el software para poder realizar las llamadas.

- Switches: algunos ejemplos de software serian “VoIPswitch”, “Mera”, “Nextone”.
- Ip-pbx: son los conmutadores. Asterisk es de los más usados y de código abierto.

2.2.3.4. Los Gatekeepers[15]

Es el software que se instala en los servidores, son el sustituto de las centralitas actuales, y el centro de toda organización VoIP. Es el primer elemento que interactúa con los terminales ya que: identifica las direcciones, traduce los números de teléfono a direcciones IP, autentica los usuarios, controla la admisión, realiza el enrutamiento…etc. para así poder establecer la comunicación entre usuarios.

2.2.3.5. Los Gateways o puertas de enlace

Es el puente de comunicación entre los usuarios, su función es la de terminar la llamada, el cliente origina la llamada y el Gateway la termina.

- Signaling Server Gateway: Es responsable del enrutamiento y la señalización del mensaje al servidor de señalización correcto.
- Media Server Gateway: Es responsable de la comunicación entre los dos extremos, controla la transmisión y los flujos de información enviados

2.2.3.6. Códec

Son especificaciones de software que se utilizan para comprimir paquetes de datos y señales.

2.2.3.7. Los protocolos de VoIP

Son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Hay muchos protocolos, señalaremos los más importantes.

2.2.3.8. Protocolos de señalización:

Son los encargados de establecer la conexión entre emisor y receptor antes de iniciar la transmisión de voz. Entre los protocolos más conocidos se encuentran:

SIP (Session Initiation Protocol), protocolo basado en el modelo Cliente-Servidor, en el que el cliente es el encargado del establecimiento y modificación de la llamada y el servidor responde y la finaliza.

Está basado en Simple Mail Transport Protocol (SMTP) y en Hypertext Transfer Protocol (HTTP).

Es un protocolo de capa de aplicación por lo que es independiente de los diferentes protocolos que utilizan paquetes como (TCP, UDP, ATM, X.25).

Destaca por su simplicidad, su modularidad, escalabilidad, integración e interoperabilidad.

SCCP (Skinny Client Control Protocol), es un protocolo propiedad de CISCO, que se utiliza para el control de llamadas cuando se cuenta con un servicio de PBX para llamar entre extensiones de una misma empresa y cuyo servidor de llamadas es el Call Manager también propiedad de CISCO.

2.2.3.9. Protocolo de comunicación:

Son el conjunto de reglas y estándares que funcionan en tiempo real para la comunicación entre los dispositivos telefónicos.

[15] También conocidos como HSS (Home Suscriber Server) o HLR (Home Location Register).

Los más utilizados son:

RTP/RTCP:

Su función principal es implementar los números de secuencia de paquetes IP para reorganizar la información de voz o video.

- Identifica los orígenes del tráfico permitiendo así, reagrupar los paquetes.
- Incorpora marcas de tiempo para poder eliminar retardos y poder detectar pérdidas.
- Reporta latencia y pérdida de paquetes.

H.323: protocolo definido por la ITU-T que determina la comunicación IP en tiempo real incluyendo audio, video e información permitiendo diferentes configuraciones para ello.

- Utiliza transporte con fiabilidad (TCP) para la señalización, por lo cual tiene una mala reputación de un alto consumo de recursos de red.
- La calidad del servicio, QoS, es manejada por (RVSP).
- Los datos son transferidos utilizando Real-Time Transport Protocol (RTP).

2.2.3.10. Protocolos de enrutamiento.

Son los protocolos para enrutar el tráfico de voz por un canal de Internet, en el cual la calidad de la voz puede ser degradada. Dentro de los principales protocolos se encuentran:

- BGP (Border Gateway Protocol).
- IBGP (Internal Border Gateway Protocol).
- OSPF (Open Shortest Path First).

2.2.3.11. Protocolos orientados a conexión

Protocolos donde las aplicaciones solicitan la conexión al destino y luego usan esta conexión para entregar los datos, garantizando que serán entregados sin problemas.

El más conocido es el protocolo TCP.

2.2.4. Tipos de arquitecturas implementadas.

La VoIP, permite que se ejecuten las redes usando una arquitectura centralizada o distribuida.

- *Arquitectura centralizada*, es aquella en la que la administración, la red, el provisionamiento y el control de llamadas es centralizado, está asociada a los protocolos MGCP y MEGACO.
- *Arquitectura distribuida,* es aquella en que, al establecer llamadas, el enrutamiento, provisionamiento, facturación o cualquier otro aspecto de manejo de llamadas se distribuye entre los dispositivos de control de llamadas y endpoints. Está asociada a los protocolos H.323 y SIP.

2.3. Ventajas y Desventajas de utilizar VoIP

Ventajas:

- Facilitar muchos procesos y servicios que normalmente son muy difíciles y costosos de implementar usando la tradicional red de voz PSTN.
- Convertir la voz, en paquetes (formato digital), que se pueden controlar, comprimir, direccionar y manipular mediante bits.
- Mayor velocidad
- Transmitir más de una llamada sobre la misma línea telefónica, lo que significa que se pueden incrementar las líneas telefónicas sin tener que poner líneas físicas adicionales.
- Integrar otros servicios disponibles como: videoconferencia, mensajes instantáneos…
- Enrutar automáticamente las llamadas a un teléfono VoIP
- Reducir los costes telefónicos y de mantenimiento.
- Desarrollar una única red que se encargue de cursar todo tipo de información.

Desventajas:

- Estar exenta a amenazas, ataques y vulnerabilidades.
- Baja calidad de llamada.
- Al transmitir información dividida en paquetes, éstos pueden perderse y no hay garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación.

3. La calidad de servicio al usuario.

La calidad de servicio es el efecto global del requisito de funcionamiento de un servicio, que determina el grado de satisfacción de los usuarios.

Hemos comentado que este trabajo está centrado en analizar qué parámetros definen la calidad del servicio en VoIP y cómo medirlos, porque los problemas de audio en VoIP, suelen deberse a desvíos en la calidad mínima exigible a problemas de calidad de servicio o de ancho de banda insuficiente.

Antes de adentrarnos en la medición de los parámetros de calidad, que deben ser objetivos y comprobables, analizaremos la calidad del servicio y porqué viene influenciada.

La carencia de calidad viene motivada por:

- El cliente, entendemos como cliente, a su red interna e infraestructura.
- Internet, que, al ser un sistema basado en conmutación de paquetes, hace que la información no viaje siempre por el mismo camino.

Conocer estos problemas y sus posibles soluciones nos hará disfrutar de mayor calidad de VoIP.

También se tiene que mencionar que los criterios que hemos considerado en la calidad de un servicio de comunicación son los que están incluidos en la recomendación ITU-T G.100, donde se establece una matriz[16] que sirve para identificar los criterios de QoS que todo servicio debe soportar, pero esta matriz se puede ver des de diferentes perspectivas según:

- Las necesidades de QoS del cliente.
- La QoS ofertada por el proveedor del servicio.
- La QoS conseguida.
- La calificación de la QoS por parte del cliente.

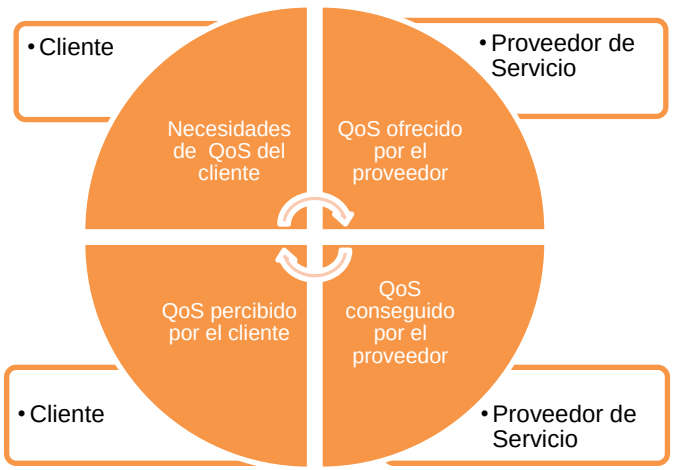


Figura 3:1 Perspectivas sobre los criterios de QoS

[16] Matriz indexada en los anexos.

3.1. Factores que afectan al QoS

- La Infraestructura de red del usuario.
- Parámetros mesurables:
  - Jitter o variación en el retardo.
  - Latencia
  - Retardos
  - Pérdida de paquetes o packet loss.
  - Eco
  - Variaciones en la velocidad y ancho de banda de la red.

3.1.1. Infraestructura de red de usuario cliente

3.1.1.1. Red interna del usuario

Según como tenga estructurada la red el usuario podemos encontrar ciertas configuraciones que afectan al funcionamiento de la VoIP y su calidad. Entre ellas están:

Los Firewalls si no están bien configurados pueden impedir que dos equipos se conecten, impidiendo la comunicación. Por eso es importante que los puertos TCP/UDP, que se estén utilizando para la VoIP, estén bien configurados.

El Router y el SIP-ALG[17]: Si queremos realizar una llamada a una extensión IP que están en otra red LAN[18], es necesario realizar la conexión a través del router, que está configurado con NAT[19] y es en este caso que aparece un problema con el protocolo SIP.

El SIP-ALG es un componente de software integrado en el propio router con NAT, que gestiona y modifica el contenido del protocolo SIP, cambiando su dirección IP y puerto del paquete haciendo que el paquete original se corrompa y provoque una mala calidad en la comunicación.

3.1.1.2. Conexión de red

El ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS).

Para lograr calidad en la comunicación VoIP, se debe tener un canal dedicado o ancho de banda garantizado de esta forma se evitan las congestiones en la red y la pérdida de paquetes. La correcta elección del códec facilita la optimización del ancho de banda.

Causas:

El ancho de banda de las comunicaciones es limitado y suele estar compartido por numerosas aplicaciones (web, correo electrónico, tráfico FTP, descarga de archivos…), eso hace que no tengamos suficiente capacidad para mantener correctamente una comunicación de voz IP.

[17] Para más información consultar anexos.
[18] LAN - Local Area Network
[19] NAT - Network Access Translation,

Valores recomendados:

El ancho de banda está estrechamente relacionado con el códec o codificación que estemos usando. Pero generalmente una conversación full-dúplex (donde ambos extremos pueden hablar y escuchar a la vez) consume no más de *22kbps.*

Posibles Soluciones:

Aumentar el ancho de banda de las redes por las que circulen nuestras comunicaciones (normalmente pagando más).

Reducir el consumo que hagan otras aplicaciones del ancho de banda (especialmente las descargas de archivos mediante redes de intercambio).

3.1.2. Parámetros de medida de la QoS

En este apartado explicamos cuales son los parámetros de medida de la QoS, definimos el parámetro, unas posibles causas, unos valores estándar[20] y unas posibles soluciones, pero es en el capítulo 4, y en el informe que generamos para el cliente donde veremos los valores reales y se harán una serie de recomendaciones para poder optimizar estos valores.

3.1.2.1. Pérdida de Paquetes[21]

Es una medida cuantitativa de la pérdida de la información sobre una conexión de red. Aunque la pérdida de paquetes sea inevitable en cualquier ambiente de red, el objetivo es siempre identificar donde se han perdido los paquetes durante la transmisión, para reducir al mínimo la pérdida de la información. Si ocurre una gran pérdida de paquetes durante una conversación telefónica, la comunicación se hará muy difícil.

Causas:

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo, no está orientado a conexión, si se produce una pérdida de paquetes no se reenvían. La pérdida de paquetes también se puede producir por descartes de paquetes que no llegan a tiempo al receptor.

La voz es bastante predictiva, si se pierden paquetes aislados se puede recomponer de una manera bastante óptima.

Valores Recomendados:

La pérdida de paquetes máxima admitida para que no se degrade la comunicación deber ser *inferior al 3%.*

Posibles Soluciones:

Una técnica eficaz para evitar la pérdida de paquetes en redes con congestión o de baja velocidad es no transmitir los silencios, ya que gran parte de las conversaciones están llenas de momentos de silencio.

Si solo transmitimos cuando haya información audible liberamos bastante los enlaces y evitaremos fenómenos de congestión.

[20] Según los detallados en la tabla del anexo determinados en la itu-t G1000.
[21] O packet Loss en inglés.

3.1.2.2. Retardos

Puede ocurrir que los paquetes tarden en alcanzar su destino. Bien porqué pueden permanecer en largas colas bien porque tomen una ruta menos directa para prevenir la congestión de la red. En algunos casos, los retardos excesivos pueden inutilizar aplicaciones tales como VoIP.

Valores Recomendados:

Los retardos en un sentido tienen que ser preferiblemente de *150 milisegundos* y como máximo admitido *400 milisegundos*.

3.1.2.3. Latencia[22]

Es una medida del tiempo que transcurre en completar una transferencia de información entre el emisor y el receptor. Este tiempo se mide en milisegundos.

La latencia de red excesiva puede causar tanto huecos sensibles como una pérdida de sincronización en conversaciones transmitidas. Si los huecos se hacen bastante grandes, los interlocutores pueden encontrar que ellos, sin querer, se interrumpirán el uno al otro.

Causas:

La suma de varios retardos que ocurren en el proceso de propagación, transmisión y procesamiento de los paquetes en la red y a lo largo de los enlaces por los que pasa el tráfico de voz.

La asignación de prioridades de paquetes, dándole la máxima prioridad al tráfico de voz, hará que una parte importante de ese tiempo disminuya, como por ejemplo el tiempo en que un paquete está en cola.

Valores Recomendados:

En VoIP la latencia debería ser inferior a los *100 milisegundos*, y se considera una latencia alta si supera los *200 milisegundos*.

Posibles Soluciones:

La latencia no es de fácil solución, ya que a veces depende de los equipos por los que pasan los paquetes, es decir, de la misma red. Podemos reservar un ancho de banda de origen a destino o señalizar los paquetes con valores de TOS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad.

Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda, aumentar la velocidad del enlace o priorizar esos paquetes dentro de nuestra red.

3.1.2.4. Jitter

Se define técnicamente como la variación en el tiempo en la llegada de los paquetes.

Causas:

La congestión de la red.

[22] También conocida como delay.

La pérdida de sincronización debida a las distintas rutas seguidas por los paquetes para llegar al destino.

Los tiempos de espera en la cola para ser transmitidos los paquetes.

Valores Recomendados:

Un jitter aceptable para comunicaciones de telefonía, se encuentra *por debajo de los 20 milisegundos.*

Posibles Soluciones:

La solución es la utilización del "jitter buffer". Consiste en asignar a los paquetes un almacén o cola, con un leve retraso, donde se reordenan y se les da tiempo a los paquetes más lentos a llegar y se descartan cuando sea necesario.

Un aumento del buffer implica menos perdida de paquetes, pero más retraso. Una disminución implica menos retardo, pero más pérdida de paquetes. La calidad de la conversación mejora, pero en cambio se incrementa la latencia total.

3.1.2.5. Eco o reverberación

Es una reflexión retardada de la señal acústica original.

Causas:

El eco puede producirse por la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el micrófono.

Valores recomendados:

Es tolerable que el eco llegue a *65 milisegundos* y *una atenuación de 25 a 30 dB*.

Posibles soluciones:

Los supresores de eco, que evitan que la señal emitida sea devuelta convirtiendo por momentos la línea full-dúplex en una linea half-dúplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario.

Canceladores de eco, es el sistema por el cual el dispositivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido).

3.2. Tabla resumen de valores

A continuación se muestra una tabla resumen de los valores anteriormente enumerados, la mayoría son valores recomendados por la ITU-T en el ámbito de las comunicaciones de voz, por lo tanto, estos valores pueden variar según la tecnología: voz, datos, video…etc.

Hay un parámetro que enumeramos pero que no hemos comentado, el MOS (mean opinión score), se trata de una medida subjetiva que cuantifica el impacto que tiene en el usuario la presencia de fallos en el servicio de en voz sobre IP, la han cuantificado como indicamos seguidamente.

Parámetro	Valores Recomendados	Satisfacción
MOS (Mean Opinion Score)	[1 – 3.6) (3.6 – 4) (4 - 4.5)	No aceptable Permitida Nivel deseado
Retardo (bidireccionalmente)	Mayor de 400ms Entre 150ms y 400ms Menor de 150ms	No aceptable Permitido Nivel deseado
Latencia	Mayor de 250ms Entre 100ms y 250ms Menor de 100ms	No aceptable Permitido Nivel deseado
Jitter	Mayor de 350ms Entre 20ms y 30ms Menor de 20ms	No aceptable Permitido Nivel deseado
Pérdida de paquetes	Hasta un 3%	Nivel permitido
Ancho de banda	100 Mb/seg	Mínimo

Tabla 3:1 Valores de los parámetros de QoS

3.3. Claves para garantizar la QoS

- Un buen conocimiento de nuestra infraestructura red, ya sea como proveedor o como usuario.
- Como cliente saber las limitaciones que tenemos.
- Como proveedor, conocer los parámetros que afectan a una red VoIP y en consecuencia tener un plan de implantación y estudio de las redes a las que se quiere implantar la VoIP.

4. Auditoría de una red VoIP

Hasta ahora hemos hablado de la VoIP y de los factores que afectan a la calidad, para conocer qué datos debemos analizar. Este capítulo se centrará en cumplir nuestro objetivo, describir un método para poder realizar una Auditoria de una red VoIP desde que un potencial cliente se plantea contratar este servicio hasta que se le instala.

4.1. Cómo enfocamos una auditoria de VoIP

Si conocemos los problemas y cómo podemos solucionarlos de la manera más eficaz y eficiente, generar el informe final será muy sencillo.

Primero debemos conocer las necesidades del cliente. La infraestructura de red tanto de la empresa como del cliente, para saber qué equipos y componentes la forman. Una vez conocida la red, debemos tener claros los parámetros que afectan a la calidad de la voz IP[23], para poder estudiar las herramientas que nos facilitaran medir la calidad del servicio y poder decidir qué herramienta es la más adecuada para llevar a cabo la auditoría.

Esquema para realizar la auditoría.

Figura 4:1 Proceso de auditoría de red

Pasos a seguir durante el proceso de auditar la red de un cliente. Se especifican en la siguiente figura:

[23] Estudiados en el capítulo 3.

Figura 4:2 Pasos a seguir durante la auditoría.

4.2. Necesidades del cliente

Preguntas que debemos hacernos para saber si un cliente podrá utilizar VoIP.

- ¿Qué servicio necesita?
- ¿Cuántas llamadas simultáneas realizará?
- ¿Terminales?
- ¿A qué se dedica el cliente?
- ¿Cuáles son las tendencias de crecimiento?

No es lo mismo que un cliente tenga 2 terminales IP que 250 tampoco es lo mismo que sea un solo cliente o estemos hablando de un Call center que realizan muchas llamadas simultáneas. Ni que el cliente utilice mucho ancho de banda para subir archivos porque el hecho de subir archivos afectará a la calidad.

4.3. Infraestructura de red del cliente

- Topología de red, equipos de red, sistemas de comunicación, aplicaciones, cableado estructurado entre otros, routers/ switches…
- ¿Qué servicios tiene contratados?
- ¿Ancho de banda disponible? ¿Ancho de banda necesario?

  Nota: Por un lado, VoIP necesita suficiente ancho de banda para funcionar con una calidad razonable. Por otro lado, VoIP va a disminuir el ancho de banda disponible para las aplicaciones de datos
- Tiene contratado: ¿Internet, fibra, ADSL…?
- ¿Qué aplicaciones y conversaciones consumen el ancho de banda? ¿Qué aplicaciones debo priorizar? ¿Cuáles consumen más ancho de banda?
- ¿Qué flujos de tráfico puedo eliminar?

4.4. Infraestructura de red de Tpartner

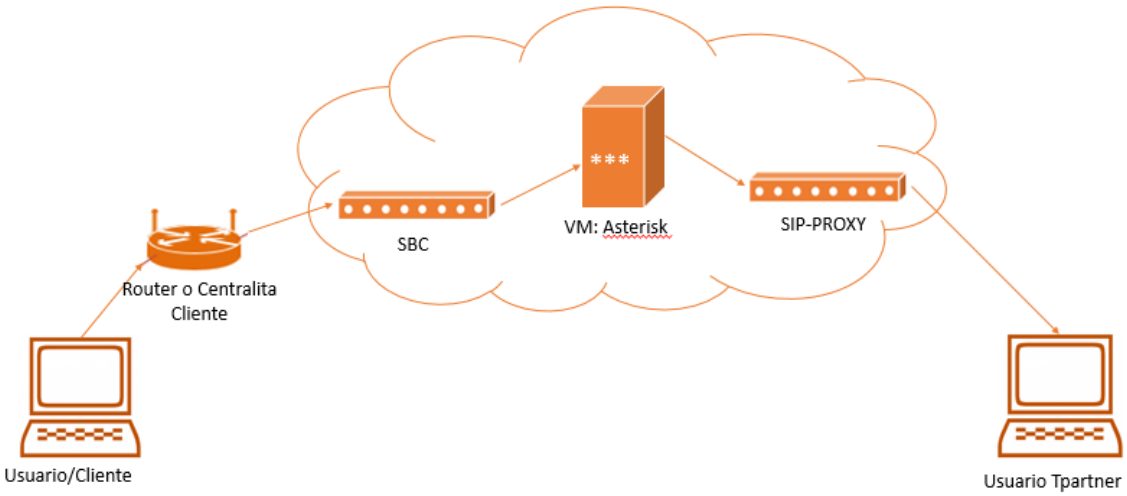


Figura 4:3: infraestructura de elementos físicos de Tpartner[24].

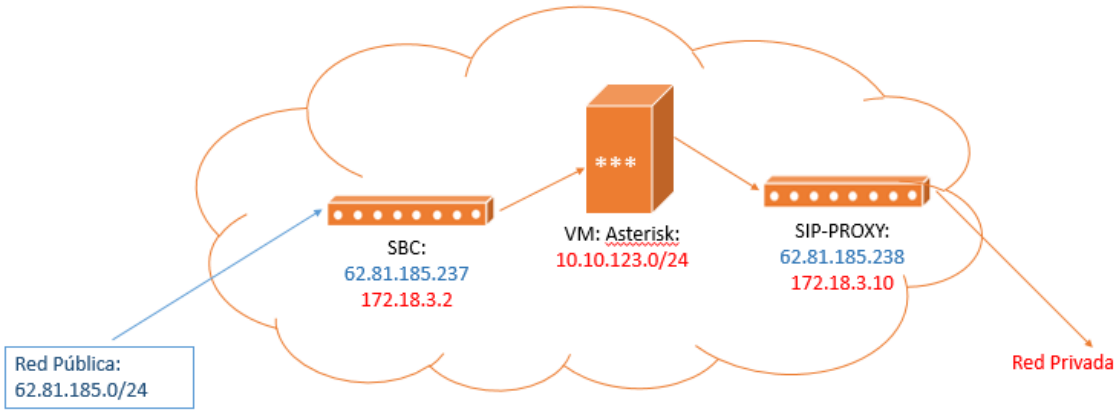


Figura 4:4 infraestructura de red de Tpartner[25]

[24] Para entender todos los elementos de red y sus funciones mirar anexos.
[25] En los anexos se puede encontrar información más detallada sobre los elementos: SBC, Proxy SIP..Etc.

4.5. Pruebas a realizar y las herramientas de las que disponemos[26].

4.5.1. Test para conocer el ancho de banda.

Para conocer el ancho de banda real del cliente, utilizaremos un test de velocidad. En Internet encontramos varias herramientas, de todas ellas hemos seleccionado dos test de velocidad diferentes, porque con una prueba nunca es suficiente.

http://www.testdevelocidad.es/

Figura 4:5: Resultado del test de velocidad 1.

http://www.speedtest.net/

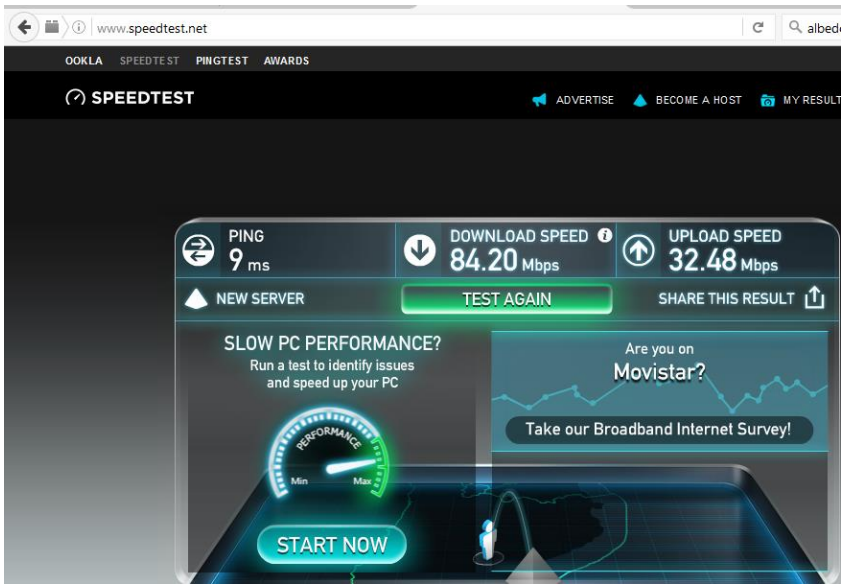


Figura 4:6 Resultado del test de velocidad 2.

[26] Para conocer mejor las características y el funcionamiento de las herramientas, consultar los anexos.

4.5.2. Ping

Es una herramienta de diagnóstico de redes, que nos ofrece información útil sobre nuestra conexión y nuestro equipo.

Si al hacer ping no obtenemos respuesta, éste será el primer indicador de que tenemos algún filtro a nivel de router o de firewall.

Comando: ping 62.81.185.237 -n 5

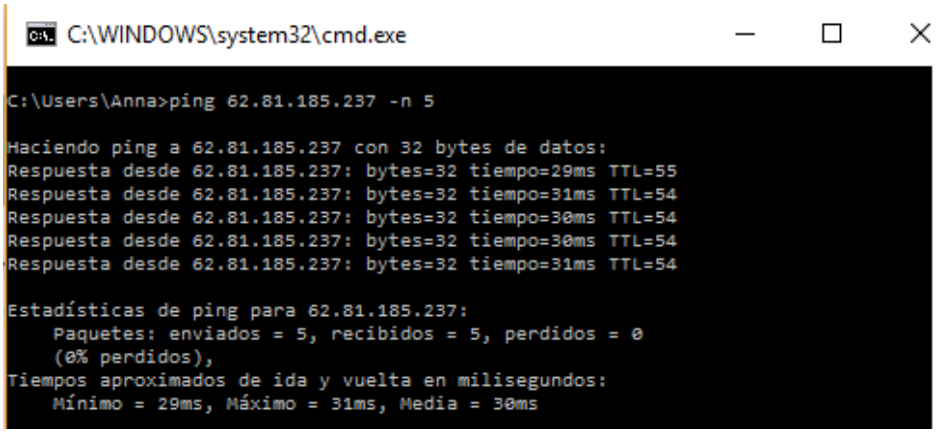


Figura 4:7 Ping por parte del cliente a la red de Tpartner, al SBC.

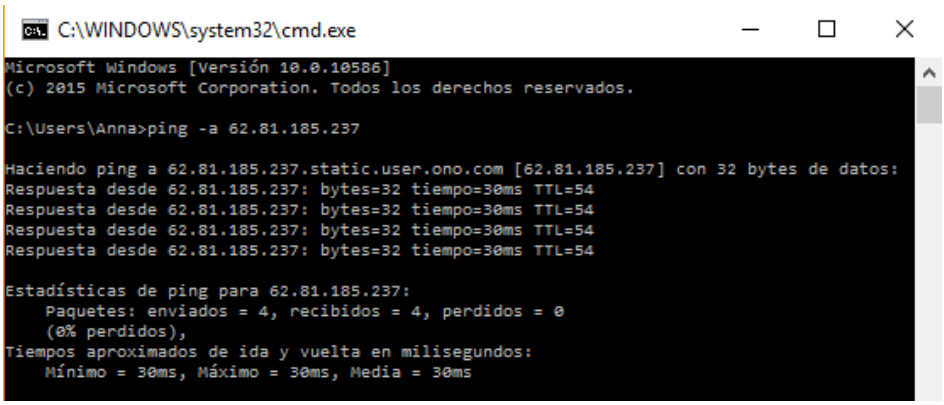


Figura 4:8 Ping para conocer el nombre asociado a la IP.

Ahora generamos carga de red con la opción -l, y como hemos perdido todos los paquetes hacemos “tracert” para ver la ruta que recorren los paquetes de datos hacia el servidor remoto y la demora de esa ruta.

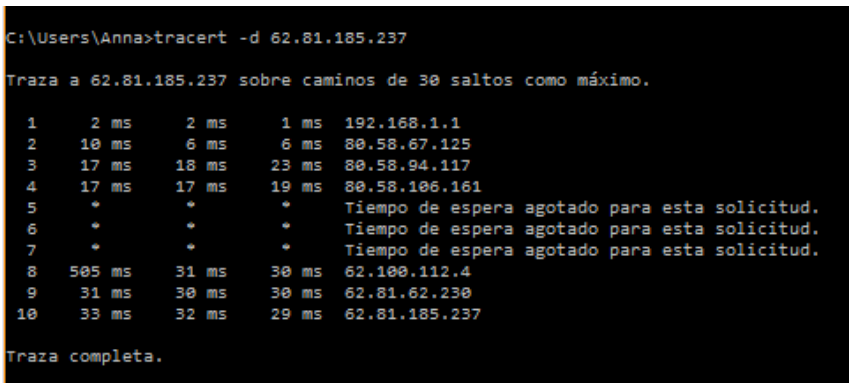


Figura 4:9 Tracert.

4.5.3. Ipconfig

Nos indica la IP del equipo, la máscara de subred y la IP del Gateway. Con esta información conoceremos la IP que tiene asignada nuestro ordenador y podremos saber si estamos en la misma red a la que nos queremos conectar.

Comando: ipconfig

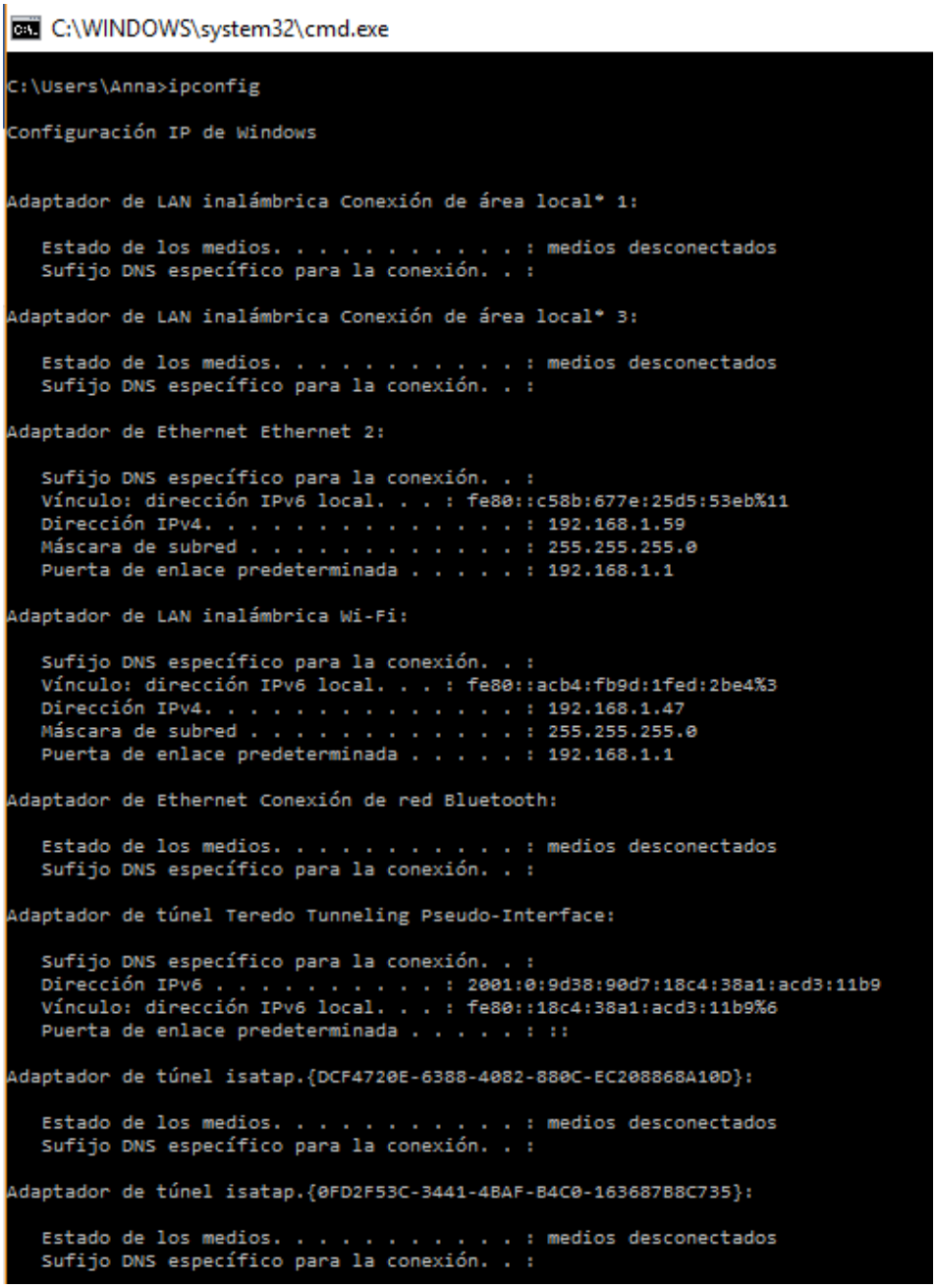


Figura 4:10 IP config de Windows

4.5.4. Netstat

Muestra el estado de la pila TCP/IP en el equipo local.

```
C:\Users\Anna>netstat -a 62.81.185.237

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:445            Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:5357           Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:6646           Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:7680           Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49664          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49665          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49666          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49667          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49668          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:49669          Lenovo-PC:0            LISTENING
  TCP    0.0.0.0:57621          Lenovo-PC:0            LISTENING
  TCP    127.0.0.1:4370         Lenovo-PC:0            LISTENING
  TCP    127.0.0.1:4371         Lenovo-PC:0            LISTENING
  TCP    127.0.0.1:4380         Lenovo-PC:0            LISTENING
  TCP    127.0.0.1:4381         Lenovo-PC:0            LISTENING
  TCP    127.0.0.1:50498        Lenovo-PC:50499        ESTABLISHED
  TCP    127.0.0.1:50499        Lenovo-PC:50498        ESTABLISHED
  TCP    192.168.1.47:139       Lenovo-PC:0            LISTENING
  TCP    192.168.1.47:45837     Lenovo-PC:0            LISTENING
  TCP    192.168.1.47:51766     mad06s10-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.47:51994     msnbot-191-232-139-99:https  ESTABLISHED
  TCP    192.168.1.47:52049     sto3-accesspoint-a10:4070  ESTABLISHED
  TCP    192.168.1.47:52070     msnbot-191-232-139-89:https  ESTABLISHED
  TCP    192.168.1.47:52107     wm-in-f125:5222        ESTABLISHED
  TCP    192.168.1.47:52109     mad06s25-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.47:52110     mad06s25-in-f141:https  CLOSE_WAIT
  TCP    192.168.1.47:53379     132.245.50.66:https    ESTABLISHED
  TCP    192.168.1.47:53605     mad01s25-in-f206:https  ESTABLISHED
  TCP    192.168.1.47:53613     mrs04s09-in-f193:https  ESTABLISHED
  TCP    192.168.1.47:53616     wl-in-f189:https       ESTABLISHED
  TCP    192.168.1.47:53621     161.69.165.24:https    ESTABLISHED
  TCP    192.168.1.47:53622     mrs04s10-in-f228:https  TIME_WAIT
  TCP    192.168.1.47:53625     mrs04s10-in-f228:https  ESTABLISHED
  TCP    192.168.1.47:53626     mrs04s09-in-f3:https   ESTABLISHED
  TCP    192.168.1.47:53629     mad01s26-in-f174:https  ESTABLISHED
  TCP    192.168.1.47:53643     a104-126-84-34:http    TIME_WAIT
  TCP    192.168.1.47:53645     151.101.12.84:http     TIME_WAIT
  TCP    192.168.1.47:53646     151.101.12.84:http     TIME_WAIT
  TCP    192.168.1.47:53647     151.101.12.84:http     TIME_WAIT
  TCP    192.168.1.47:53648     151.101.12.84:http     TIME_WAIT
  TCP    192.168.1.47:53649     151.101.12.84:http     TIME_WAIT
^C
C:\Users\Anna>
```

Figura 4:11 Netstat

4.5.5. SIP ALG

Como ya hemos comentado en el capítulo anterior y en los anexos se detalla, el SIP ALG del router lo tenemos que desactivar. Para ello, debemos conocer la marca del router y desactivarlo manualmente según se indique en el manual, el proceso de desactivación de cada router es diferente. Por ejemplo:

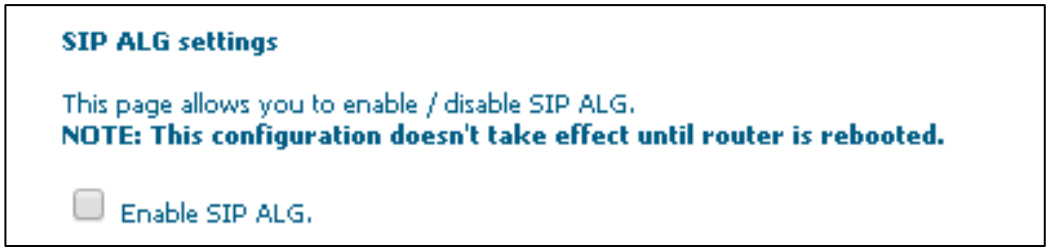


Figura 4:12 Ejemplo de habilitar/deshabilitar SIP ALG en página web movistar.

4.5.6. Wireshark y SNGrep

Realizado el test de velocidad, el ping y desactivado el SIP ALG del router del cliente, por tanto, comprobada que la red del cliente es apta para todas las prestaciones de la VoIP

El primer paso para poder auditar la red será definir dónde analizar el tráfico. Lo analizaremos tanto en la parte del cliente como en la de Tpartner, para comprobar que lo que emite el usuario se recibe sin ningún fallo.

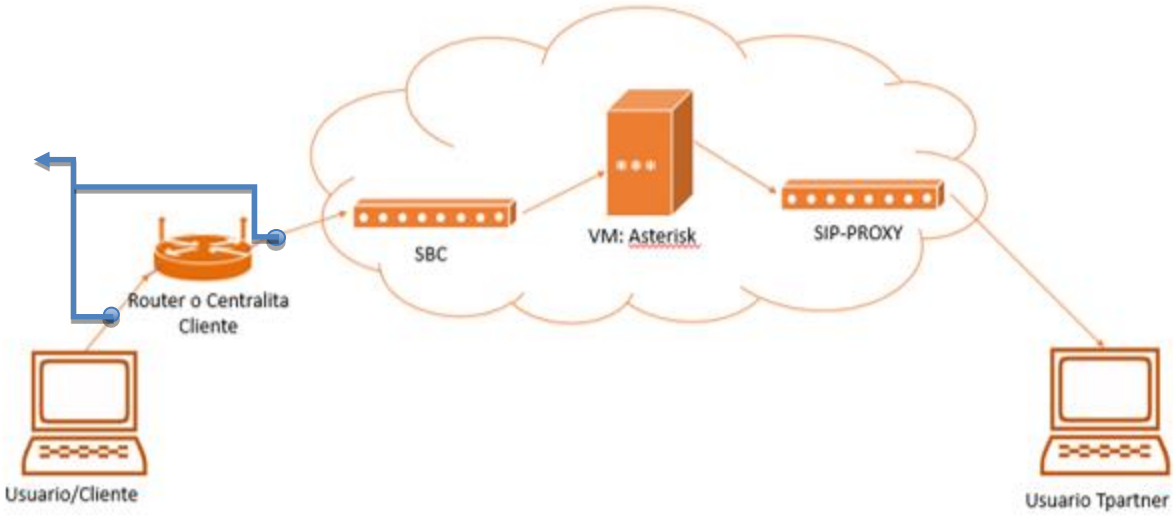


Figura 4:13 En azul, puntos donde ejecutaremos el análisis.

Wireshark es un capturador y analizador de tráfico, protocolos y redes open-source que incluye una interfaz gráfica, y cuyo principal objetivo es la captura del tráfico de red para analizar las trazas de comunicación. Permite escuchar las conversaciones, analizar audio y monitorizar distintas llamadas entre muchas otras funcionalidades.

Como en VoIP debemos centrarnos en analizar los paquetes SIP, en Wireshark utilizaremos un filtro para visualizar sólo los paquetes y protocolos que nos interesan.

Complementariamente a Wireshark utilizaremos **Sngrep**, un capturador y visualizador de paquetes SIP, que nos permitirá ver fácilmente una llamada y los mensajes que se intercambian entre sí. Se implementa directamente desde la consola de Linux, analiza el tráfico en tiempo real y nos permite seleccionar capturas en formato *.pcap*, que después podemos analizar en Wireshark.

Ejemplo del análisis de una llamada con tráfico:

Para analizar una llamada telefónica, hemos puesto funcionando el Wireshark a la vez, tanto en el ordenador del cliente, que ha generado la llamada, como en la red de Tpartner durante la misma llamada, para comprobar que lo paquetes que se emiten son los mismos que se reciben.

Desde el punto de vista del usuario:

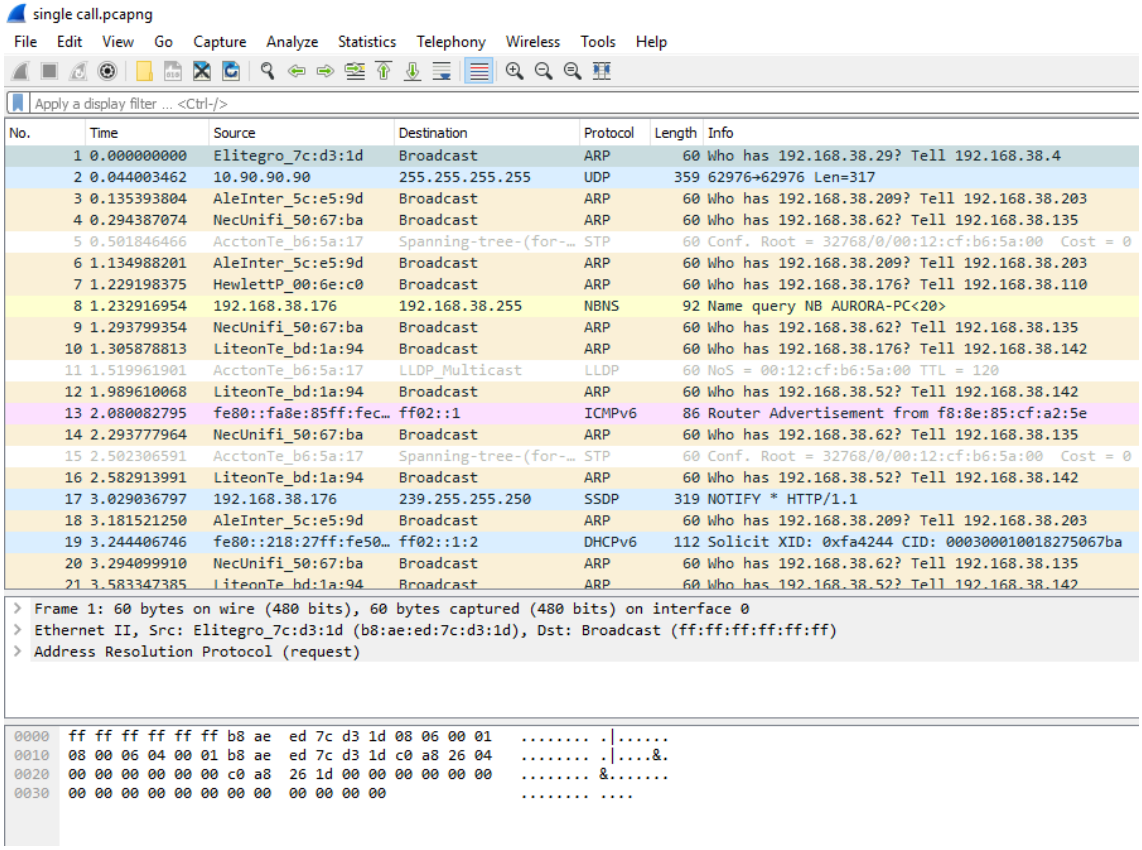


Figura 4:14 Toda la captura de tráfico.

- Ponemos un filtro en el Wireshark para que estén solo visibles los paquetes SIP, que son los que contienen la voz:

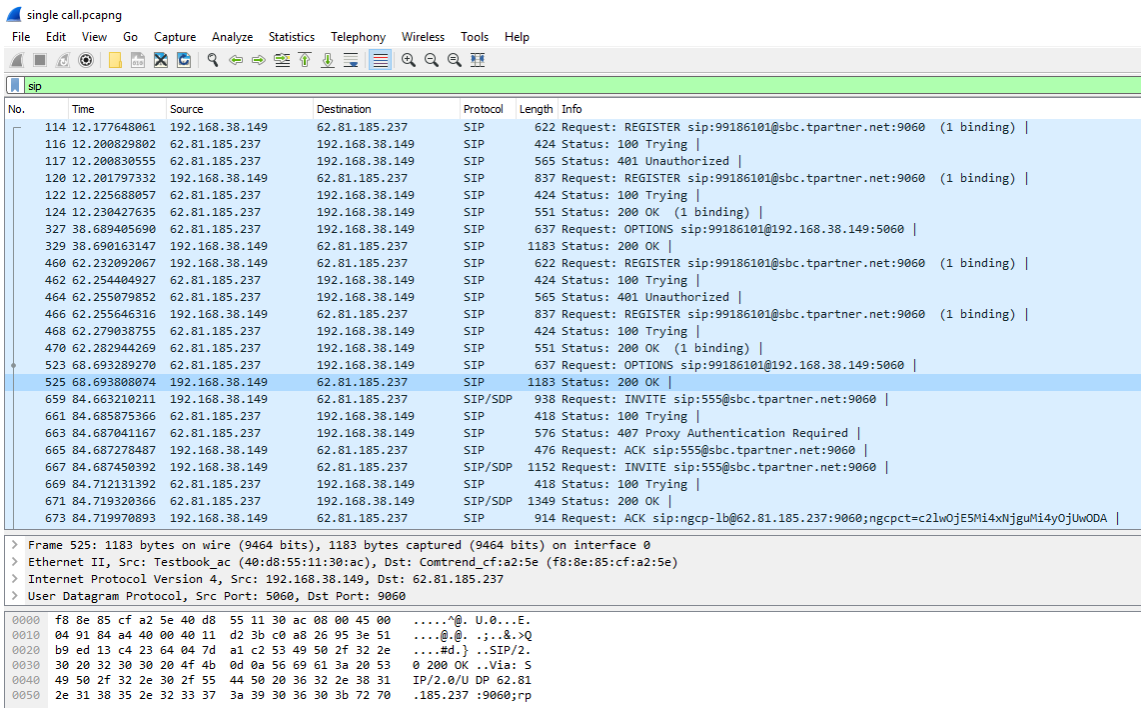


Figura 4:15 Tráfico SIP

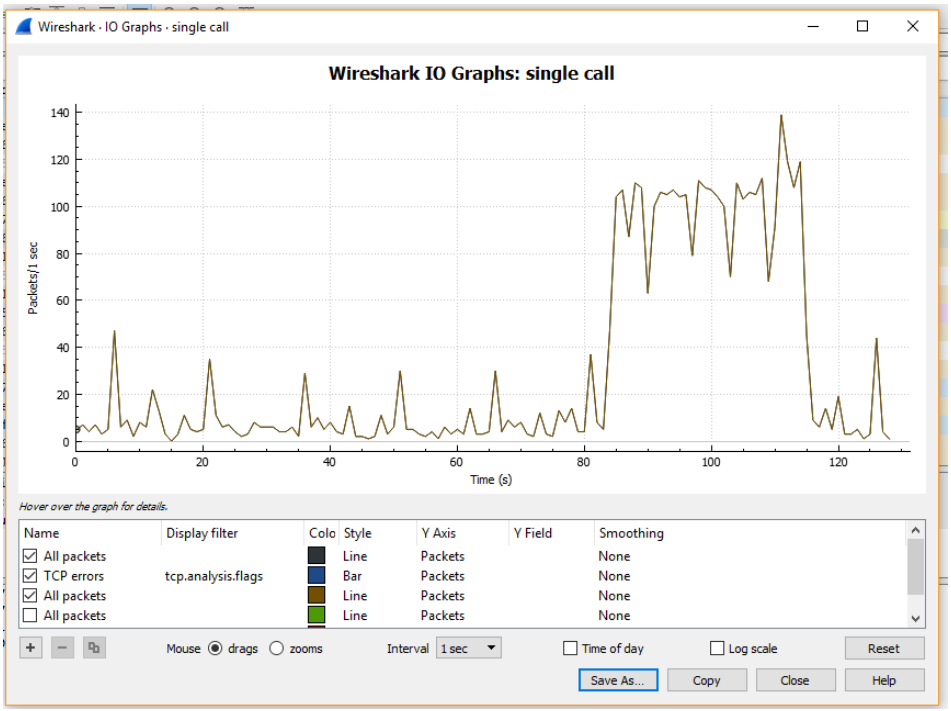


Figura 4:16 Gráfico del tráfico que ha habido durante la llamada.

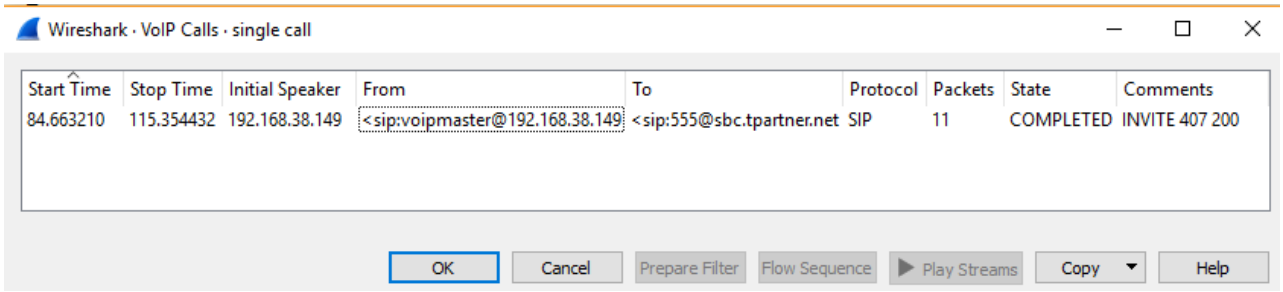


Figura 4:17 Llamada generada.

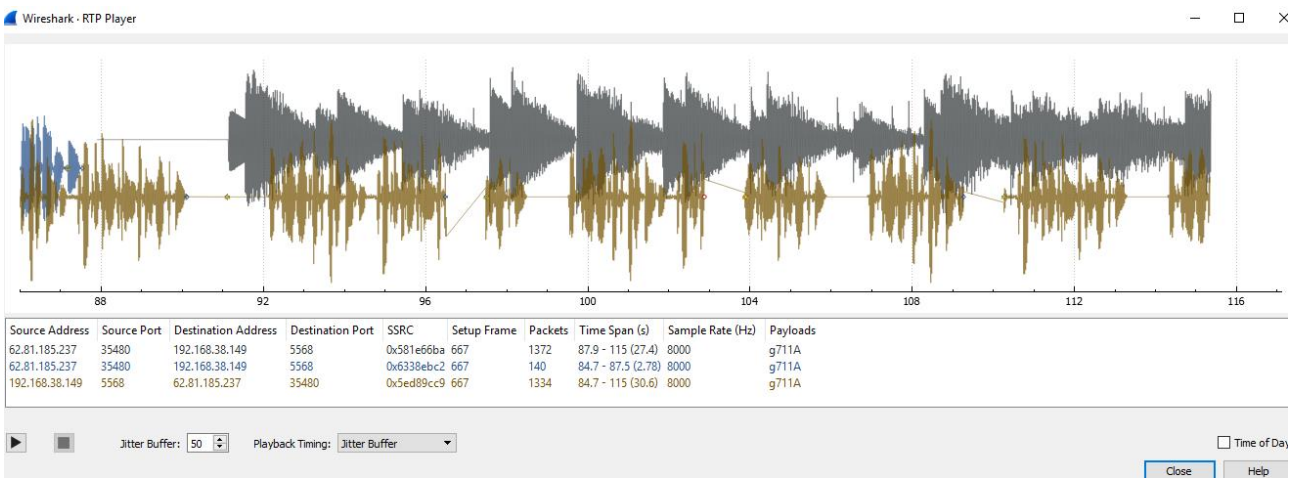


Figura 4:18 Reproducción de la llamada.

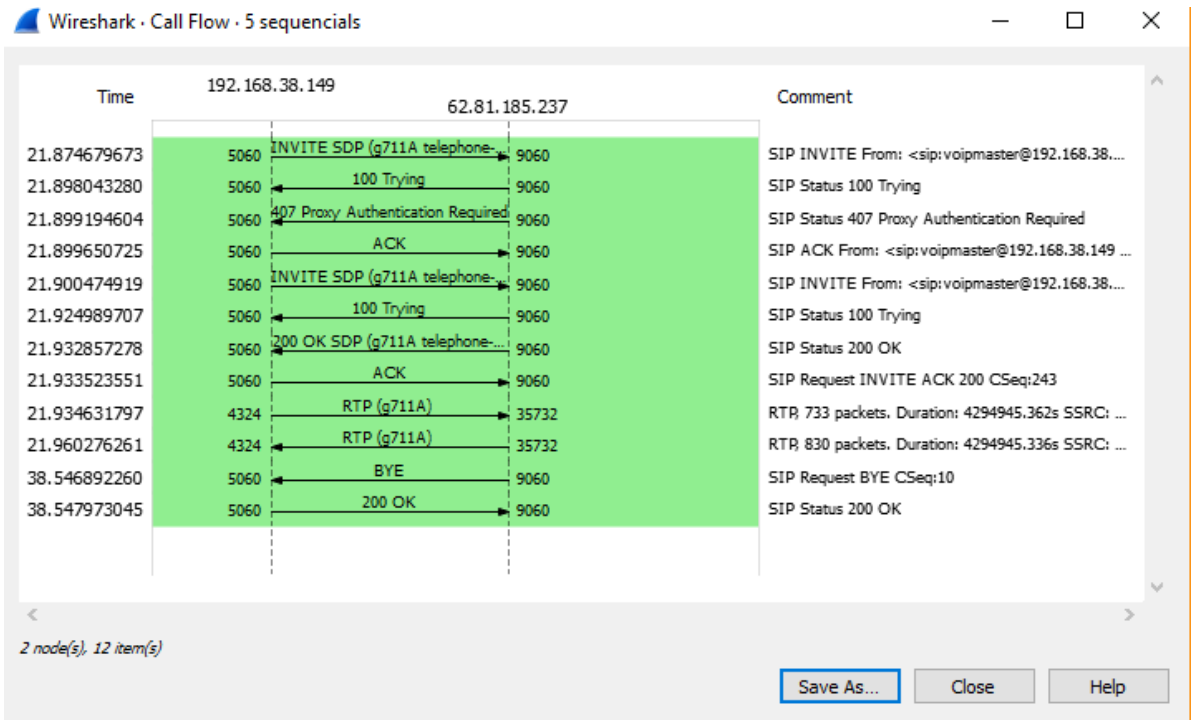


Figura 4:19 Flujo de la llamada generada por el cliente.

Desde el punto de vista de Tpartner:

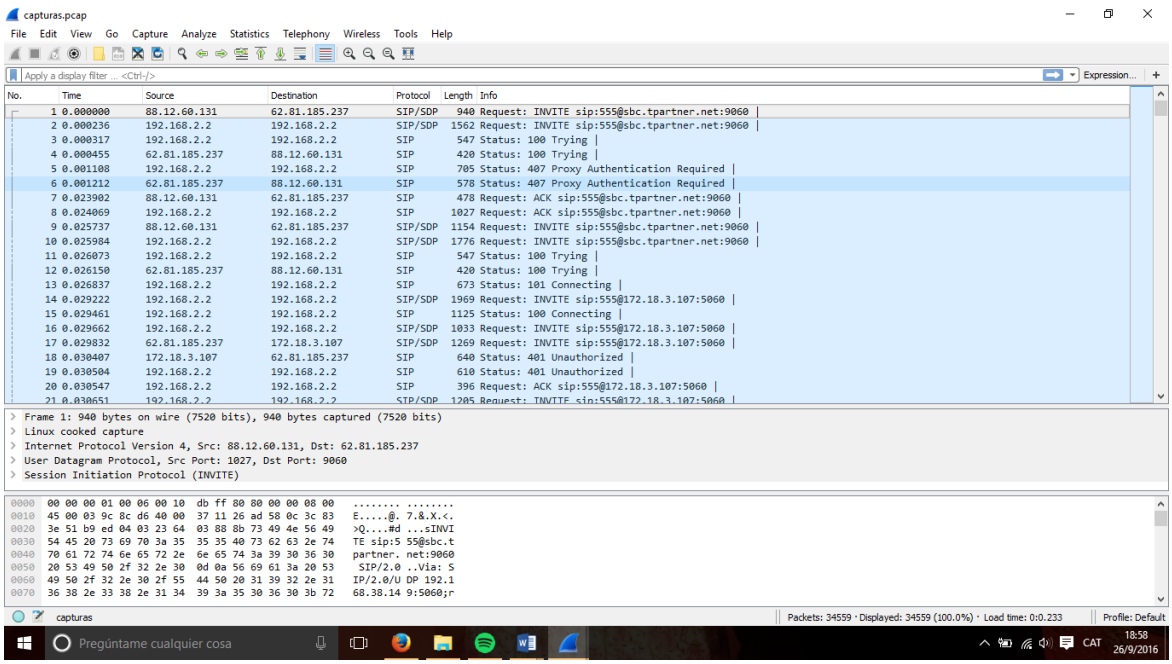


Figura 4:20 Tráfico SIP captado en el SBC de Tpartner

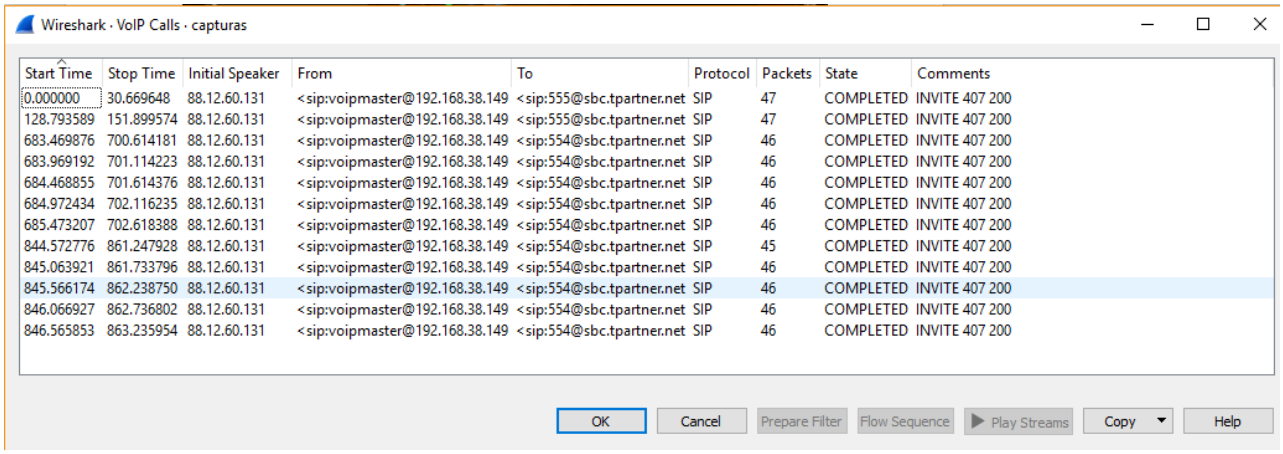


Figura 4:21 Llamadas de VoIP captadas.

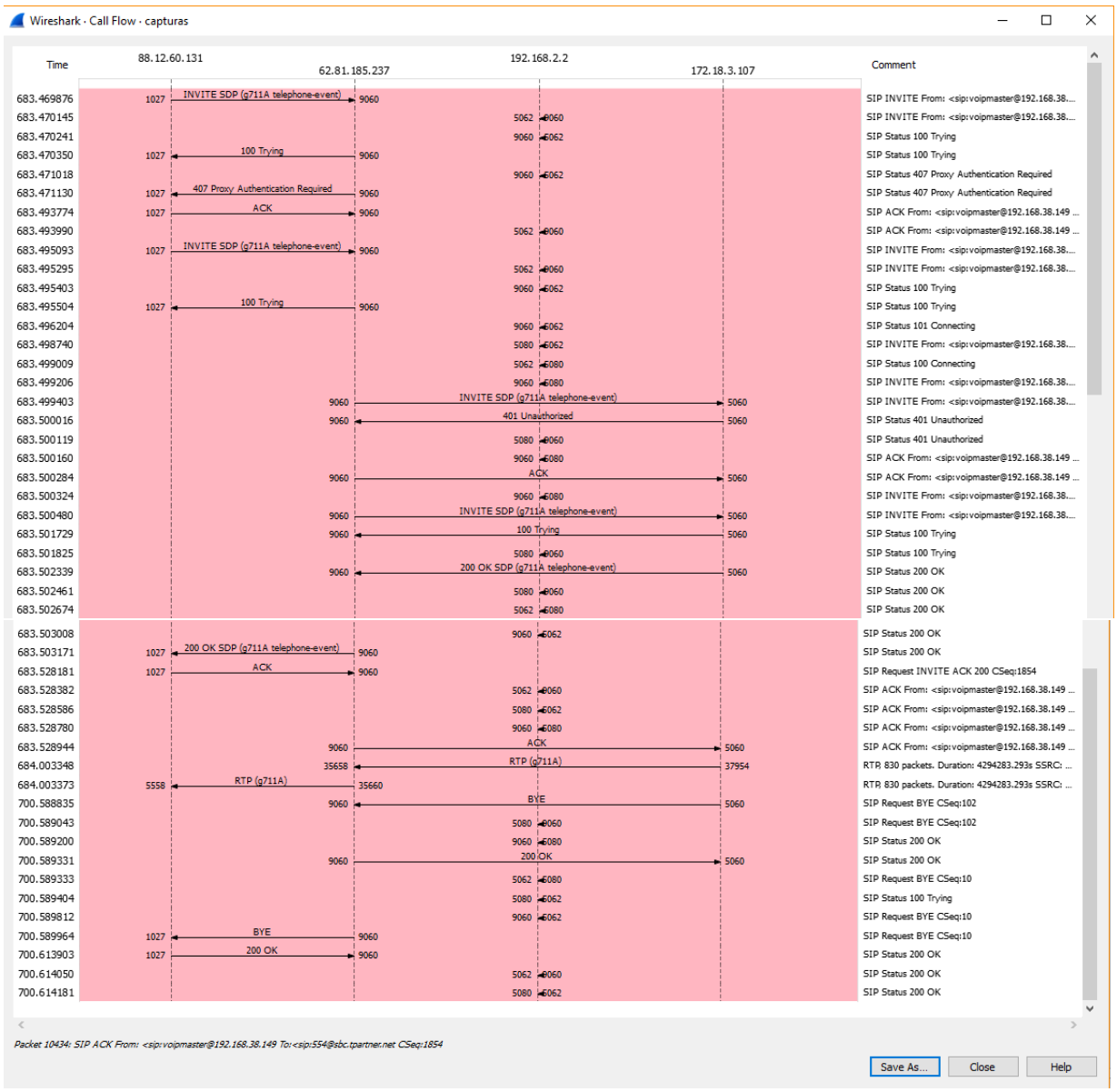


Figura 4:22 Flujo de la llamada.

- Por parte de Tpartner he sido capaz de extraer todas las capturas y archivos .pcap para posteriormente poder analizarlos con Wireshark, a continuación muestro el flujo de llamadas que se pueden observar directamente con Sngrep sin necesidad de extraer los archivos e ir llamada a llamada para comprobar cuál es la que nos interesa analizar.

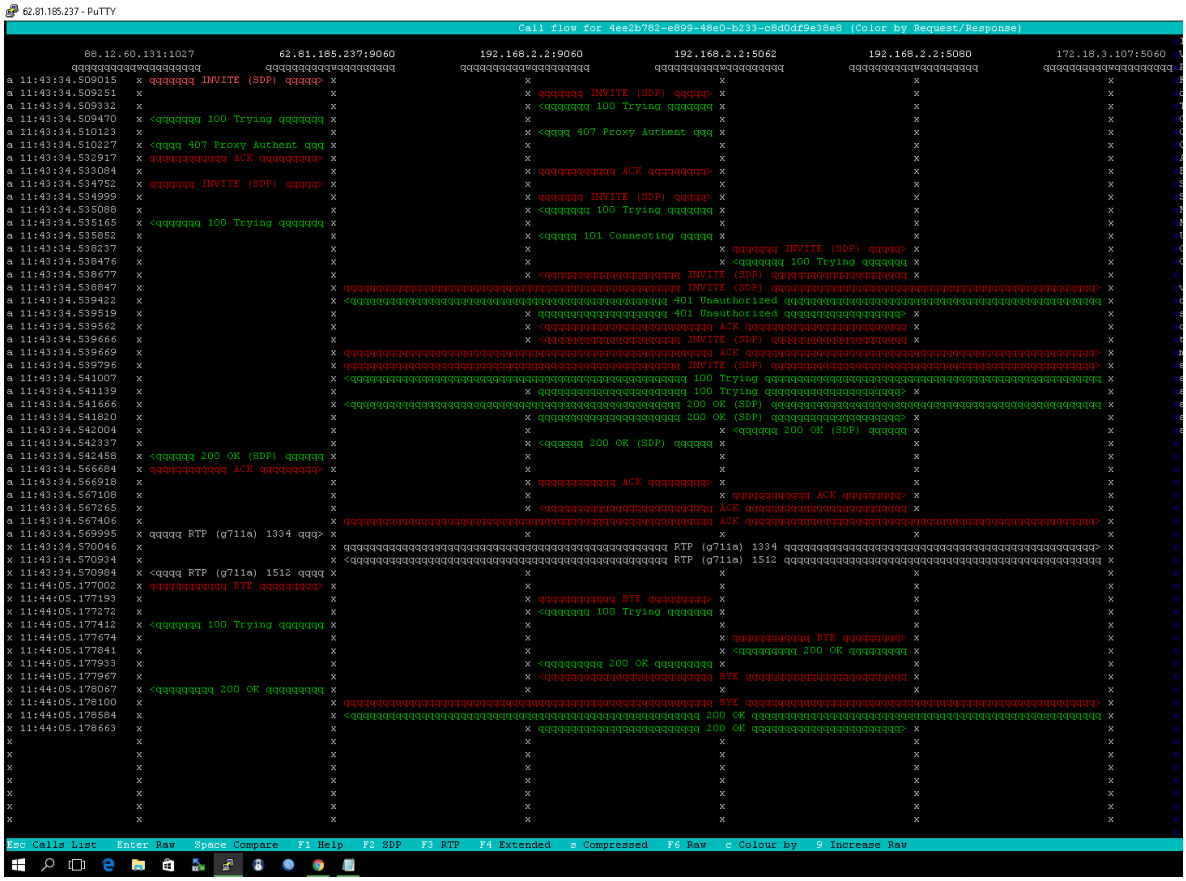


Figura 4:23 Flujo de llamada con Sngrep

Wireshark y Sngrep, son herramientas muy completas para el análisis de las comunicaciones VoIP, tienen muchas funcionalidades y opciones, pero no son suficientes para proporcionar al cliente un informe sobre los problemas de su red, porque no sería capaz de interpretar los gráficos. Es un problema que nos hemos encontrado y por eso que nos vimos obligados a buscar alternativas para generar el informe. Tras un proceso de búsqueda y comparación de diferentes herramientas nos decantamos por *VoIP master.*

4.5.7. VoIP master[27].

Nos hemos decantado por *VoIP master*, como el "tester" que vamos a utilizar, porque es un software muy completo que emula desde el punto de vista del cliente o del proveedor la red donde se ejecutarán los servicios de VoIP. Pueden configurarse diferentes escenarios y medir los parámetros de calidad de una llamada y después genera un informe en formato PDF, que se entrega al cliente y le indica si su red es apta o no para la instalación de la voz IP.[28]

[27] Para profundizar en el funcionamiento de VoIP master y los informes que podemos extraer mirar anexo.

[28] Para más información sobre su funcionamiento mirar anexos y consultar la página del distribuidor del producto: http://www.albedotelecom.com/pages/emulation/src/voipmaster.php

Este tester se suministra en un pendrive “bootable” con un Linux que nos permite instalar en el ordenador del cliente, y con unas plantillas, preconfiguradas por nosotros, ejecutamos las pruebas con distintos escenarios y nos genera el informe que más tarde le será entregado al cliente.

Características:

- Hasta 30 llamadas salientes/entrantes simultáneas
- Calidad de los medios de comunicación medida (E-modelo MOS) para cada llamada.
- Informes de prueba PDF completa.
- Posibilidad de llamar a diferentes números (destinos), número de gamas etc.

A continuación, mostramos una figura con los cuatro perfiles que pueden emularse con el producto:

- Un emulador de una línea de fax.
- Una emulación PBX
- Una emulación de red SIP
- Una emulación de una llamada masiva

Figura 4:24: modos de funcionamiento de VoIP. Master

De los cuatro modos con los que se puede trabajar, los dos más interesantes para nosotros son el PBX o bien el SIP, ya que emulan la red desde el punto de vista del usuario o bien del proveedor de red respectivamente.

Pero nosotros trabajaremos con la emulación PBX, puesto que el VoIP master se ejecutará físicamente en la red del cliente.

Figura 4:25 PBX EMULATION

Figura 4:26 SIP EMULATION

Una vez configurado el sistema, y tras realizar las diferentes pruebas y tests sobre la red del cliente, podemos determinar que:

- Es importante antes de empezar a hacer pruebas, conocer las necesidades del cliente a auditar, ya que si no podemos cubrir dichas necesidades no será necesario realizar la auditoría ni ofrecerle dicho servicio.
- Una vez conocidas y concretadas las necesidades del cliente, previo a ir in situ para realizar las pruebas que nos ayudaran a generar el informe, deberemos conocer cuál es la topología de red del cliente, qué elementos la componen y qué servicio de telefonía tiene contratado.
- Cuando ya conocemos todo lo necesario acerca del cliente y sabemos de antemano que no hay ningún factor externo o limitativo que pueda influenciar en la calidad del servicio de voz IP, concretamos un día para ir a realizar las pruebas.
- Después de recopilar toda la información, se realizará y se le entregará al cliente un informe detallado acerca de si puede o no gozar del servicio de voz sobre IP.
- A partir de los resultados recopilados con las diferentes pruebas podemos señalar que:
    - Si el cliente tiene contratado un servicio de Internet de menos de 100Mb/seg, el servicio de MOS obtenido por el tester está por por debajo de 3.4 y hay una pérdida de paquetes de más del 10% la red no es apta.
    - Si el cliente tiene contratado un servicio de internet de hasta 1Gb/seg, el MOS obtenido por el tester está entre 3.4 y 3.7 y la pérdida de paquetes está alrededor del 5% pueden surgir problemas con el servicio.
    - Si el cliente tiene contratado un servicio de internet de más de 1Gb/seg, el MOS obtenido por el tester está por encima de 3.8 y la pérdida de paquetes es menor del 5% la empresa puede instalar Voz sobre IP

Una vez terminada la auditoría, el informe final será entregado cómo mostraremos en el siguiente punto.

5. Informe final[29]

[Insertar Logo Empresa]

Informe de auditoría de red.

Realizado por: Tpartner

Ref.: OXXXX

Dd/mm/AAAA

[29] El texto que está entre corchetes son las anotaciones para la persona que redactará el informe.

Presentación

Este documento agrupa toda la información necesaria por parte de Tpartner para poder realizar una auditoría de red para comprobar si **[Nombre_Cliente**] consta de la infraestructura y recursos necesarios para poder implantar la voz sobre IP.

Los objetivos de la auditoría son:

- Conocer las necesidades que tiene el cliente.
- Conocer la topología de red del cliente.
- Realizar una serie de pruebas para poder obtener las medidas de los parámetros de calidad y saber si el cliente puede optar a la solución de VoIP para su empresa.
- Generar y entregar un documento que además de informar al cliente servirá a Tpartner

En caso de requerir información adicional no duden al ponerse en contacto el personal de Tpartner:

Atentamente,

Situación actual

Necesidades del cliente:

- Servicios requeridos por parte de **Nombre_Cliente**: [*Explicar brevemente*]
- Flujo de llamadas por parte de **Nombre_Cliente**: [*Cuantas llamadas simultáneas como máximo realiza el cliente*].
- Número de extensiones y terminales que utilizará **Nombre_Cliente**: [*Poner los números].*
- Actividad que realiza **Nombre_Cliente**: [*Función que realiza la empresa, es importante saber si la tendencia de la empresa es ocupar el ancho de red y en qué lo ocupa*].
- Tendencias de crecimiento de la Empresa: [*Comentar si la empresa tiene una o varias centrales o si tiene previsto crecer a corto o largo plazo y cuál supondría el crecimiento*].

Infraestructura de red del Cliente:

Previo a la realización de las pruebas in situ en **Nombre_Cliente**, se efectuará un breve cuestionario para conocer la infraestructura del cliente.

- Servicios de telefonía e Internet que tiene contratados: [Indicar con qué compañía el cliente tiene contratados estos servicios y cuáles son].
- Velocidad de red que tiene el cliente contratado: [*Internet, fibra, ADSL e indicar la velocidad].*
- Ancho de banda: [*Averiguar o indicar de qué ancho de banda dispone y cuánto es necesario para el servicio de VoIP y para que siga funcionando Internet*].
- Aplicaciones: [*Comentar si la empresa tiene alguna aplicación que consuma gran parte del ancho de banda*].
- Topología de Red: [*Debe conocerse qué equipos forman la red del usuario y configuración tienen, para evitar posibles problemas futuros*].

Adicional: Si hay algún aspecto que se necesita comentar sobre el cliente y que puede afectar al funcionamiento de la Voz sobre IP, comentar problemas que se pueden encontrar.

Pruebas y resultados

Con todos los datos registrados y analizados previamente, y tras haber pasado una evaluación previa por parte del personal de Tpartner, si se considera que **Nombre_Cliente** cumple los requisitos para poder ofrecerle el servicio de voz sobre IP, se concretará una cita con el Cliente, y en ésta se realizarán una serie de pruebas y se registrarán los resultados, para ser enviados posteriormente al cliente.

[*En la empresa se realizarán las pruebas que se han determinado a lo largo del trabajo:*

- *Test de velocidad, que determinará el ancho de banda real de la empresa.*
- *Ping al servidor de Tpartner para comprobar que no haya ningún elemento en la infraestructura de red del cliente que interfiera en la comunicación.*
- *Comprobar que en el router esté inhabilitado el SIP ALG.*
- *Iniciar el VoIP master para:*
  - *Realizar una llamada al SBC de Tpartner y poder hacer una captura de paquetes con wireshark, tanto en la empresa como en Tpartner.*
  - *Con unos perfiles previamente configurados se ejecutarán las pruebas y se observarán los resultados obtenidos.*
  - *Las pruebas que se realizarán con VoIP master serán:*
    - *1 llamada simple al servidor*
    - *Varias llamadas simultáneas al servidor*
    - *1 llamada cuya duración será de un par de horas y se irá generando tráfico de red.*
  - *Con el VoIP master se generarán los informes automáticos sobre: Jitter, pérdida de paquetes, congestión de tráfico y sus respectivos valores.*

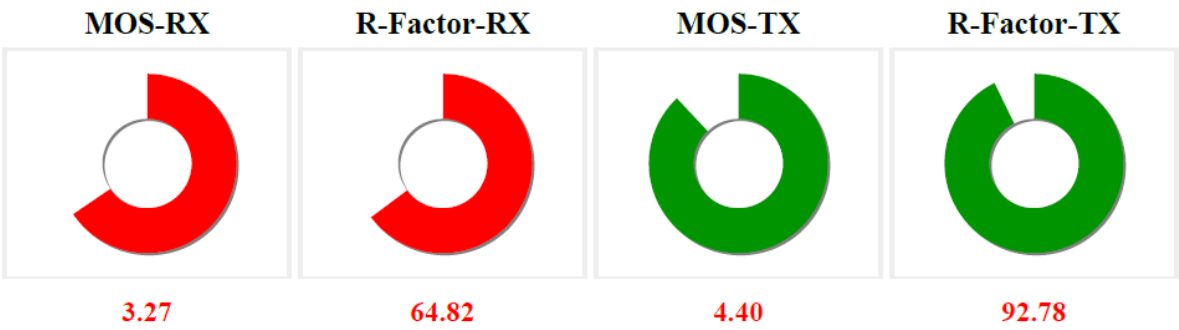
]

Valores

Tras una serie de pruebas realizadas y con la información facilitada por parte **Nombre_Cliente** podemos concluir:

- Velocidad de red real: [*insertar valor obtenido].*
- Medidas de calidad obtenidas:

[Aquí se adjuntarán una serie de imágenes obtenidas gracias a VoIP master, cuyos resultados serán analizados por el personal de la empresa cualificado, y se determinará finalmente si el usuario puede o no instalar voz sobre IP, por ejemplo:



RX	IA Jitter (ms)	RTT Delay (ms)	Loss (%)	Max Jitter (ms)	Min Jitter (ms)	Max RTT (ms)	Min RTT (ms)
	0.24	18.18	1.89	1.38	0.00	24.84	23.01

TX	IA Jitter (ms)	RTT Delay (ms)	Loss (%)	Max Jitter (ms)	Min Jitter (ms)	Max RTT (ms)	Min RTT (ms)
	0.88	24.24	0.00	1.90	0.10	24.84	23.01

Figura 0:1 Parámetros de QoS del transmisor y del receptor.

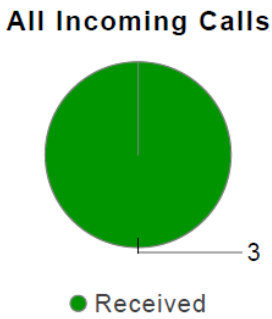


Figura 0:2 Número de llamadas correctamente recibidas durante las pruebas

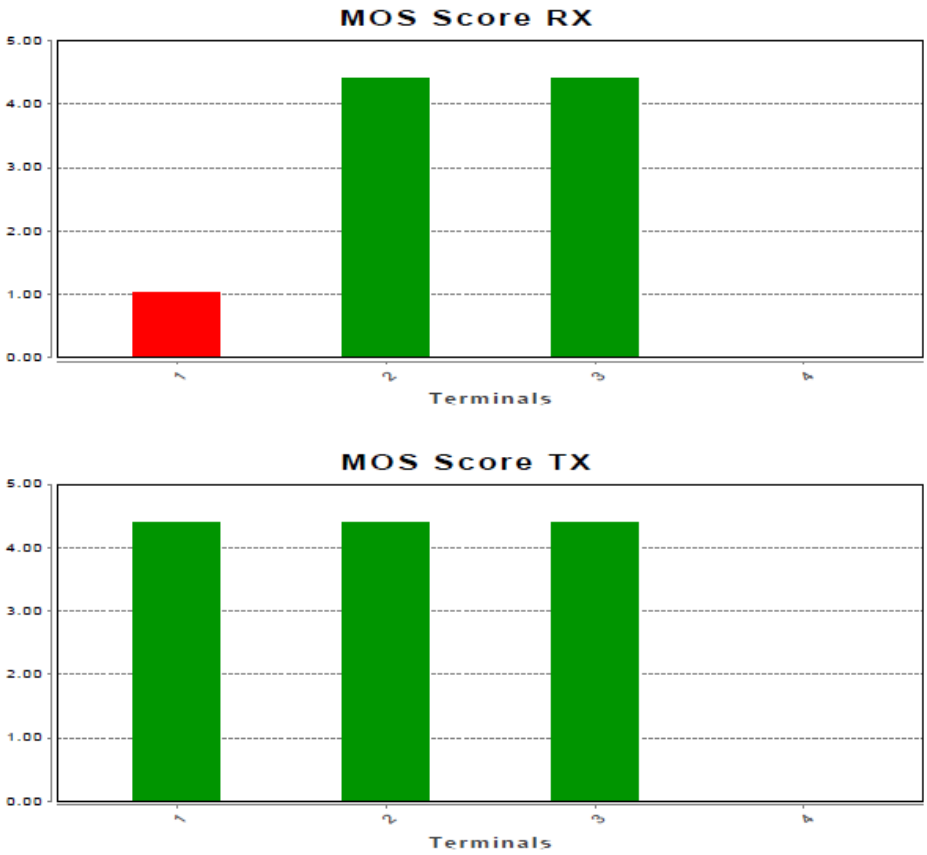


Figura 0:3 Gráficas del MOS del Emisor y Receptor

Una vez analizados los resultados y complementados con wireshark, si se determina que:

- *El MOS obtenido está por debajo de 3.4 y hay una pérdida de paquetes de más del 10% la red no es apta.*
- *El MOS obtenido está entre 3.4 y 3.7 y la pérdida de paquetes está alrededor del 5% pueden surgir problemas con el servicio.*
- *El MOS obtenido está por encima de 3.8 y la pérdida de paquetes es menor al 3% la empresa puede instalar Voz sobre IP.*

Marcar en qué estado se encuentra la red del cliente en el gráfico

]

Resultados y condiciones

[Aquí se le explicará al cliente, las pruebas realizadas, analizadas y su resultado, tanto si es satisfactorio como si no lo es, se le especificará que los resultados no siempre son exactos y que pueden variar.

Se pueden hacer una serie de recomendaciones para mejorar la calidad de red de su empresa.

Se detallará que este documento sirve para eximir a Tpartner de problemas futuros que puedan surgir con la Voz IP, en el caso de que los resultados de la auditoría hayan sido un poco problemáticos.]

6. Conclusiones

En la actualidad los servicios “tradicionales” y los nuevos servicios de VoIP coexisten. En el futuro, el mercado tiende cada vez más a la adaptación a la voz sobre IP. La garantía para poder ofrecer y percibir un buen servicio es una Auditoria de conformidad de una red con VoIP, que incluye un estudio de la red del cliente, un análisis de las características de los equipos y la generación de tráfico real de VoIP que mida los parámetros de rendimiento y de esta forma poder informar al cliente de la calidad del servicio que se le podrá ofrecer.

En este proyecto se ha logrado diseñar e implementar una metodología para llevar a cabo la auditoría y para la medición de los parámetros de red. La metodología, elaboración e implementación ha sido la adecuada porque hemos llegado al objetivo principal de este trabajo: *Generar un documento que se puede entregar a un potencial cliente informándolo de si su red es apta o no para la instalación de VoIP*.

Lo hemos conseguido mediante el estudio de todos los conceptos y componentes que forman una red VoIP, sus limitaciones y las herramientas que se disponen para poder evaluar todos los parámetros que afectan a la calidad.

Algunos inconvenientes que hemos encontrado para el desarrollo del trabajo:
La parte teórica, ya que se debe documentar y alcanzar una base técnica y teórica para poder realizar el proyecto, como sucede en la mayoría de los proyectos.
Otro inconveniente con el que a priori no contábamos, era que con las herramientas Open-Source y utilizadas a lo largo de la carrera no eran suficientes para alcanzar el objetivo, para superarlo hubo que realizar un trabajo de investigación y analizar otra herramienta para poder complementar todas las demás.

Todo el proceso se ha realizado siguiendo las etapas y cumpliendo con los objetivos señalados al principio del documento. Sin embargo, los objetivos han estado variando constantemente y siempre se han ido adaptando a las nuevas necesidades y requisitos, pero respetando los objetivos finales.

En este trabajo he desarrollado un modelo en el que he utilizado un software específico para testear la red. Los costes directos de este proyecto ascenderían a:
Una licencia del software de 750 euros más las horas dedicadas/coste ingeniero junior.

6.1. Conclusiones personales

Concluido este trabajo final de carrera mi valoración es positiva porque:

A nivel académico me ha ayudado a recuperar y refrescar conocimientos que tenía “almacenados en archivos que parecían ocultos” en el entorno de las tecnologías de redes, análisis y diseño de infraestructuras. También me ha permitido adquirir nuevos.
No hay duda que he puesto en práctica muchos de los conocimientos teóricos recibidos durante la carrera, pero lo más sorprendente ha sido comprobar cómo he interiorizando los valores que he adquirido día a día en el Campus Nord de la *Universitat Politècnica de Catalunya.* De todos resaltaría: Determinación, perseverancia, constancia, sacrificio, planificación, modo de abordar y resolver los problemas

Al ser un proyecto creado desde cero he estado aplicando las sugerencias y opiniones de mi muy apreciado tutor y los consejos y comentarios de miembros de la empresa, asumiendo las críticas constructivas que han ayudado siempre a mejorar el proyecto.

6.2. Líneas futuras

Perfeccionar y optimizar el proceso de auditoría de red para que no tener que utilizar y corroborar un mismo problema con diferentes herramientas. Probablemente queden líneas de mejora y optimización del proyecto ya que el campo de la telefonía y administración de redes es muy amplio y está en constante crecimiento y mejora.

7. Bibliografía

ALBEDO TELECOM. (2016). *VoIP.MASTER: service turn-up*. Obtenido de http://www.albedotelecom.com/products/voipmaster/voipmaster_zz_news1.html

ALI, A. A. (2004). *Voice Over IP 101: Understanding the Basic Functions, Components, and Signaling in VoIP Networks.* Sunnyvale (California, USA):: Juniper Networks, Inc. .

Boquera, M. d. (2003). *Sistemas Avanzados de Telecomunicación.* Madrid: Ediciones Díaz de Santos.

Brob, J., & Meinel, C. (8-13 de June de 2008). *Can VoIP Live up to the QoS Standards of Traditional Wireline Telephony?* Obtenido de Fourth Advanced International Conference on Telecommunications: http://ieeexplore.ieee.org/document/4545514/?reload=true&arnumber=4545514

Chua, T.-K., & Pheanis, D. (23-29 de Abril de 2006). *Effects of Loss Characteristics on Loss-Recovery Tecniques for VoIP.* Obtenido de International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies : http://140.98.202.196/xpl/mostRecentIssue.jsp?punumber=10841

CONTI, J. (2004). *Talk about a change [VoIP replacing PSTN].* Obtenido de IEEE Explore Digital Library: http://ieeexplore.ieee.org/document/1395329/?tp=&arnumber=1395329&queryText%3DTalk%20about%20a%20change%3E

E.800, I.-T. R. (23 de Septiembre de 2008). *E.800 : Definiciones de los términos relativos a la calidad de servicio*. Obtenido de https://www.itu.int/rec/T-REC-E.800-200809-I/es

G.1010, R. I.-T. (2002). *UIT-T. Serie G: Sistemas y medios de transmisión, sistemas y redes digitales. Calidad de Servicio y de transmisión.* Obtenido de https://www.itu.int/rec/T-REC-G.1010-200111-I/en

J.Hens, F., & Caballero, J. (2008). *Triple Play. Building the Convergent Network for Data, VoIP and IPTV.* Wiley.

Ministerio de indústria, energía y turismo. Calidad de Servicio. (s.f.). Obtenido de http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/CalidadServicio/Paginas/Calidad.aspx

Sinologic. (2006). Obtenido de https://www.sinologic.net/blog/

Técnicas básicas para resolver problemas y depurar llamadas VoIP. (23 de Marzo de 2008). Obtenido de http://www.cisco.com/cisco/web/support/LA/7/74/74700_voip_debugcalls.pdf

Telecomunicaciones, U. I. (2004). *Lista de recomendaciones del UIT-T*. Obtenido de https://www.itu.int/itudoc/itu-t/86097-es.pdf

UIT-G 1000, R. (29 de Noviembre de 2001). *SERIE G: SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES Calidad de servicio y de transmisión*. Obtenido de https://www.itu.int/rec/T-REC-G.1000-200111-I/es

UIT-R M, 1. (2000). *Requisitos relativos a la calidad de funcionamiento y servicio en las redes de acceso a las telecomunicaciones móviles.* Obtenido de https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1079-2-200306-I!!PDF-S.pdf

Zamorano, C. (25 de 01 de 2010). *Red Voip en un operador de telecomunicaciones.* Obtenido de http://www.coit.es/publicac/publbit/bit140/39-41.pdf

8. Anexos

8.1. Protocolo SIP

En este primer apartado del anexo, explicaremos mejor el protocolo SIP para poder entender la problemática con el router NAT y el SIP ALG que explicaremos en el punto 7.2 y que hemos comentado en el capítulo 3. También hablaremos del SIP Proxy, elemento que está presente en la infraestructura de red de Tpartner.

Como ya hemos mencionado, SIP es un protocolo de señalización, tal como indica su nombre, Session Initiation Protocol o protocolo de inicio de sesiones, que permite el intercambio de paquetes, ya sean TCP o UDP entre los usuarios y la red, pero no es el encargado del transporte. El transporte de voz o del vídeo se realiza mediante el protocolo RTP (Real Time Protocol).

Además de ser un protocolo de señalización, está dentro de la categoría de protocolos *peer to peer*, esto significa que tanto el emisor como el receptor pueden hacer la función de cliente o de servidor.

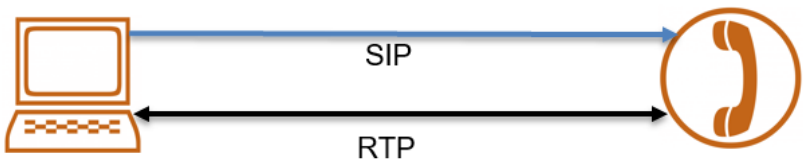


Figura 8:1 conexión SIP

SIP consta de diferentes **métodos** que describen las peticiones de los clientes.

- Invite: permite invitar a un usuario en la iniciación de una sesión o diálogo.
- Ack: confirma las respuestas, en este caso el establecimiento de una sesión.
- Options: solicita información a un cliente sobre sus capacidades, número de códecs soportados, extensiones…etc.
- Register: utilizado para registrar un cliente SIP en un SIP register.
- Cancel: cancela una petición que aún no ha sido atendida.
- Bye: indica la terminación de una sesión.

Como todo, el protocolo SIP tiene una serie de **problema**s derivados de las redes IP, concretamente debido al uso de direcciones IP privadas.

1. Problemas con los Firewalls.
    - Impiden a dos equipos SIP la recepción o envío de tráfico TCP o señalización SIP, por tanto, la VoIP mediante SIP no funciona correctamente.
    - Solución: identificar que puertos TCP/UDP deben ser abiertos, y evitar abrirlos todos, si no somos blanco de vulnerabilidades.
    - Suele ser el 5060 UDP
2. Problemas con el NAT: es un tema suficientemente importante y lo trataremos en el siguiente apartado del anexo, porqué del NAT y el SIP-ALG son conceptos que van ligados.

3. Problemas de encriptación de las comunicaciones:
    - Durante la comunicación SIP, se deben proteger tanto la señalización como el transporte de paquetes, esto se hace mediante una serie de protocolos (TLS Y SRTP), pero también provoca que no haya compatibilidad.

Alternativas a SIP: Hay otros protocolos para las comunicaciones IP, a continuación, nombramos los más conocidos y algunas de sus características.

- **H 323**: es un protocolo estandarizado por la ITU-T donde se definen los protocolos para la transmisión de audio, video y datos a través de una red IP. Pero hoy en día se ha reemplazado por SIP, ya que es menos complejo y más rápido.
- **Inter-Asterisk Exchange Protocol by Asterisk (**IAX2**)**: es un protocolo utilizado por Asterisk para controlar conexiones VoIP entre servidores y clientes que utilizan este mismo protocolo, minimiza el ancho de banda y evita problemas de NAT, por ello está gozando de popularidad.
- **Skinny Client Control Protocol by Cisco (SCCP)**: es un protocolo propiedad de CISCO utilizado en sus sitemas de Call Manager y en sus terminales telefónicos.

SIP Proxy, es un servidor cuya función es la de redirigir paquetes SIP sin que la carga sea un problema.

- Cuando recibe un paquete de una dirección IP, lo reenvía a otra distinta.
- Registra y actualiza la localización de los dispositivos SIP.
- Se encarga de responder a un usuario cuando realiza una llamada a un dispositivo SIP que está apagado.

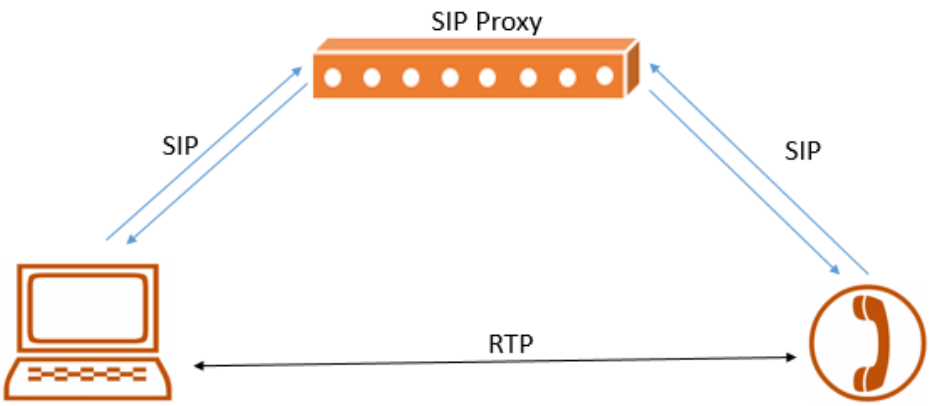


Figura 8:2 Conexión con SIP Proyx

Como se observa en la figura anterior la transmisión de los contenidos RTP se realiza directamente entre los equipos sin utilizar el SIP Proxy, ya que las tramas de voz tienen una carga elevada y como el protocolo SIP es un protocolo ligero, el SIP proxy puede atender la señalización de miles de llamadas por segundo.

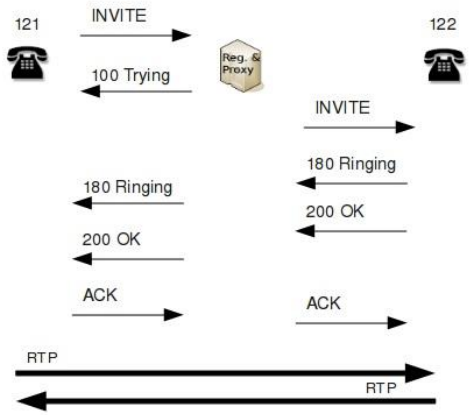


Figura 8:3 Ejemplo de una comunicación SIP:

Previo a cualquier comunicación es necesario que los equipos estén registrados en el SIP proxy.

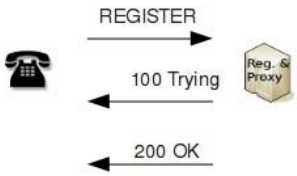


Figura 8:4 Solicitud de registro al servidor proxy.

8.2. NAT

El NAT, Network Address Translation en inglés, es un mecanismo integrado en los routers, que se encarga de traducir las direcciones IP de una red privada a direcciones IP públicas.

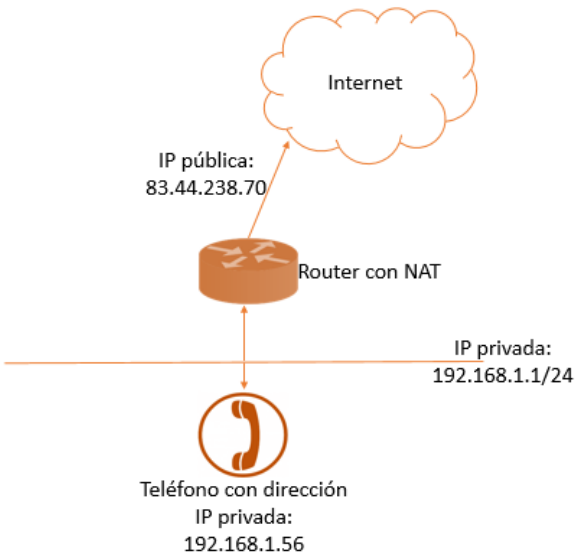


Figura 8:5 Esquema de Router con Nat

Es una funcionalidad útil pero las conexiones de voz sobre IP son incompatibles con NAT. Esto implica varios problemas en las comunicaciones a través de SIP cuando el router tiene activado el NAT:

- Si queremos generar una llamada con nuestros teléfonos IP que están dentro de una LAN con direcciones IP son privadas a otras extensiones que están dentro de otra red LAN, es necesario establecer la comunicación a través del router con NAT, pero éste impide la entrada de cualquier paquete que no sea una respuesta a una petición realizada previamente desde la red interna.

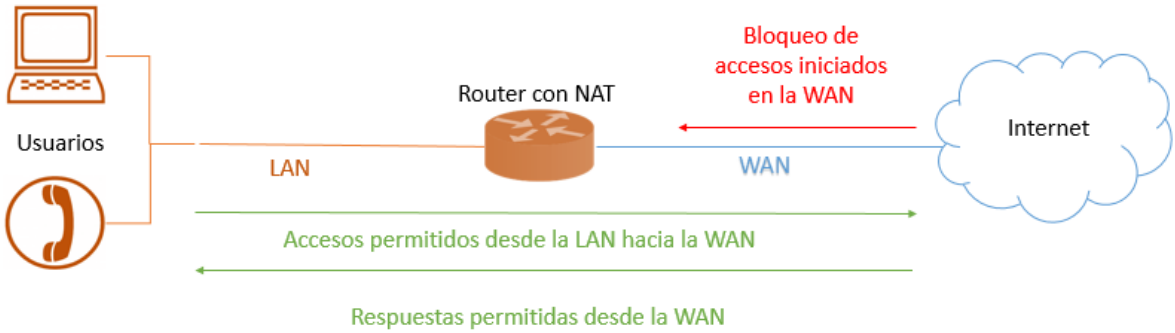


Figura 8:6Accesos y respuestas durante una comunicación con router Nat.

- Dos teléfonos IP no pueden intercambiar paquetes de voz a través de la WAN utilizando las IP privadas, deben ir dirigidos hacia las IP públicas de la WAN de los routers y aunque un paquete RTP se dirija hacia la IP pública no pasará a través del NAT si previamente no ha habido una conexión saliente a través he dicho NAT.

Resumiendo, por un lado, los paquetes RTP no pueden dirigirse a una IP privada y por el otro, aunque se modifique la dirección IP privada por su IP pública, cuando los paquetes RTP se dirijan al router extremo del receptor no podrán atravesar el NAT si previamente no ha habido una conexión saliente que establezca una asociación IP privada-puerto/IP pública-puerto en el router.

Actualmente los routers utilizan el SIP ALG (Application Level Gateway), una función que viene habilitada por defecto y soluciona los problemas derivados del NAT pero modifican el encabezado y cuerpo de los paquetes de voz incorrectamente, rompiendo el protocolo SIP y haciendo imposible la comunicación con el servidor. Por esta razón se tiene que deshabilitar el SIP ALG.

8.3. SBC

El SBC o Session Border Controler es un firewall orientado al tráfico de voz, su función es garantizar que las comunicaciones de voz que se establecen entren la red interna y externa son seguras y fiables, detectando y bloqueando posibles ataques y vulnerabilidades, así como ocultar la red interna de cara al exterior.

El SBC se sitúa entre el firewall y la red Interna, para tener control total sobre las sesiones de red, así si se quiere establecer una sesión desde la red interna a la externa, primero se establece entre el teléfono de la red interna y el SBC y después del SBC a la red externa.

Características y funciones:

- Asegurar el establecimiento de sesiones.
- Gestión del plan de numeración.
- Adaptación de códec
- Control de admisión
- Se encarga de la conectividad de usuarios remotos.

Por esto hoy en día la mayoría de operadores y proveedores de VoIP incorporan el SBC en su infraestructura de red.

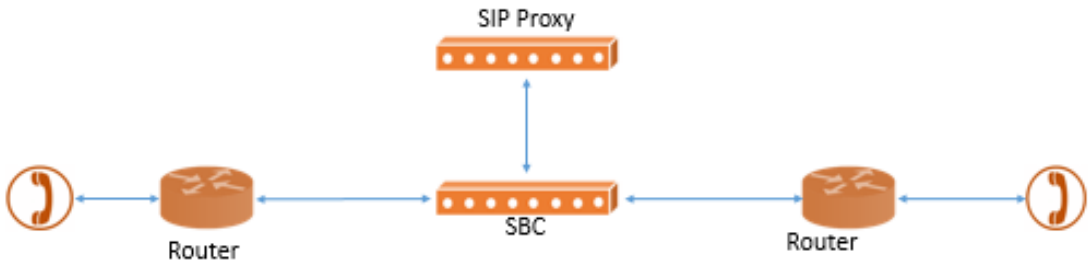


Figura 8:7 Esquema de la posición del SBC en una comunicación

8.4. Matriz calidad del servicio según UIT-T G.1000 (11/2001)

			Criterios de calidad de servicio						
			Velocidad 1	Precisión 2	Disponibilidad 3	Fiabilidad 4	Seguridad 5	Simplicidad 6	Flexibilidad 7
Función de servicio									
GESTIÓN DE SERVICIO	Ventas y actividades precontractuales	1							
	Prestación	2							
	Alteración	3							
	Atención al cliente	4							
	Reparaciones	5							
	Cese	6							
CALIDAD DE LA CONEXIÓN	Establecimiento de conexión	7							
	Transferencia de información	8							
	Liberación de conexión	9							
Facturación		10							
Gestión de la red/el cliente	servicio por	11							

Fuente: UIT-T

Figura 8:8 Matriz para facilitar la identificación de los criterios de QoS para las comunicaciones.

8.5. Cuadro Anexo 1I.1/G.1010

Cuadro I.1/G.1010 – Objetivos de calidad de funcionamiento para aplicaciones audio y vídeo

Medio	Aplicación	Grado de simetría	Velocidades de datos típicas	Parámetros clave y valores de objetivo para la calidad de funcionamiento			
				Tiempo de transmisión en un sentido	Variación de retardos	Pérdida de información (Nota 2)	Otros
Audio	Voz en conversación	Dos sentidos	4-64 kbit/s	Preferido < 150 ms (Nota 1) Límite < 400 ms (Nota 1)	< 1 ms	Relación de pérdida de paquete (PLR) < 3%	
Audio	Mensajería vocal	Principalmente en un sentido	4-32 kbit/s	< 1 s para reproducción < 2 s para grabación	< 1 ms	PLR < 3%	
Audio	Audio en tiempo real de gran calidad	Principalmente en un sentido	16-128 kbit/s (Nota 3)	< 10 s	<< 1 ms	PLR < 1%	
Vídeo	Videoteléfono	Dos sentidos	16-384 kbit/s	Preferido < 150 ms (Nota 4) Límite < 400 ms		PLR < 1%	Sinc. labios: < 80 ms
Vídeo	Un sentido	Un sentido	16-384 kbit/s	< 10 s		PLR < 1%	

NOTA 1 – Se supone el control de eco adecuado.

NOTA 2 – Los valores exactos dependen del códec específico, pero se supone el uso de un algoritmo de ocultación depérdida de paquete para minimizar el efecto de esa pérdida.

NOTA 3 – La calidad depende mucho del tipo de códec y de la velocidad binaria.

NOTA 4 – Estos valores se consideran valores de objetivo a largo plazo y es probable que la tecnología actual no los satisfaga.

Figura 8:9 Objetivos de calidad de funcionamiento para aplicaciones de audio y vídeo.

8.6. Ping

Ping (Packet Internet Groper) es un comando o herramienta de diagnóstico que permite comprobar mediante un equipo el estado de una determinada conexión de un host o servidor. Lo hace mediante paquetes de solicitud ECO y Respuesta al ECO (Echo Request y Echo Reply).

- Es útil para diagnosticar los errores de redes o enrutadores IP.
- Muchas veces se utiliza para medir la latencia o tiempo que tardan en
- comunicarse dos puntos remotos.
- El comando ping funciona de la misma forma para windows y para linux, pero cuando se necesita ingresar parámetros varía en sus letras
- Un ping de más de 100 milisegundos supone una pérdida de comunicación.

Se suele utilizar tecleando en la línea de comandos:

ping *IP_del_otro_pc*

Lo que se verá en la pantalla es una respuesta mostrando la cantidad de bytes que se están enviando y el tiempo que se demora en dichos paquetes.

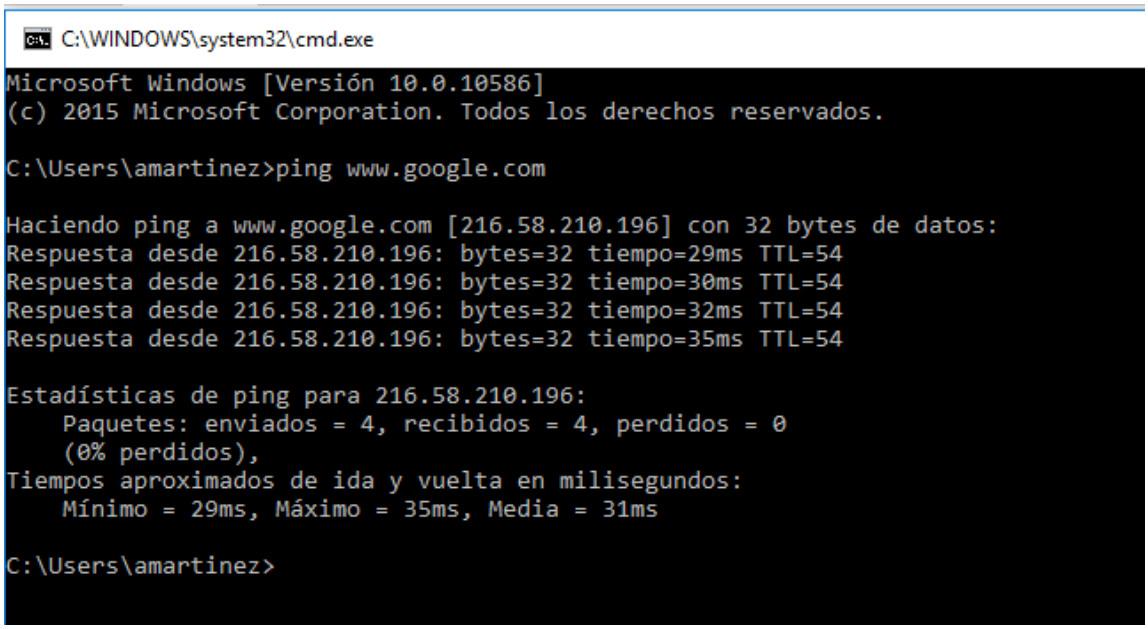


Figura 8:10 Ejemplo de ping en Windows

8.6.1. Windows:

Uso:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list] [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p] [-4] [-6] nombre_destino

Opciones:

-t	Hacer ping al host especificado hasta que se detenga. Para ver estadísticas y continuar, presione Ctrl-Interrumpir; para detener, presione Ctrl+C.
-a	Resolver direcciones en nombres de host.
-n count	Número de solicitudes de eco para enviar.
-l size	Enviar tamaño de búfer.
-f	Establecer marca No fragmentar en paquetes (solo IPv4).
-i TTL	Período de vida.
-v TOS	Tipo de servicio (solo IPv4. Esta opción está desusada y no tiene ningún efecto sobre el campo de tipo de servicio del encabezado IP).

-r count	Registrar la ruta de saltos de cuenta (solo IPv4).
-s count	Marca de tiempo de saltos de cuenta (solo IPv4).
-j host-list	Ruta de origen no estricta para lista-host (solo IPv4).
-k host-list	Ruta de origen estricta para lista-host (solo IPv4).
-w timeout	Tiempo de espera en milisegundos para cada respuesta.
-R	Usar encabezado de enrutamiento para probar también la ruta inversa (solo IPv6). Por RFC 5095 el uso de este encabezado de enrutamiento ha quedado en desuso. Es posible que algunos sistemas anulen solicitudes de eco si usa este encabezado.
-S srcaddr	Dirección de origen que se desea usar.
-c compartment	Enrutamiento del identificador del compartimiento.
-p	Hacer ping a la dirección del proveedor de Virtualización de red de Hyper-V.
-4	Forzar el uso de IPv4.
-6	Forzar el uso de IPv6.

Tabla 8:1 Comandos Windows de ping

8.6.2. LINUX

Uso:

ping - send ICMP ECHO_REQUEST packets to network hosts

ping [-aAbBdDfhLn0qrRUvVmqw] [-c count] [-F flowlabel] [-i interval] [-I interface] [-l preload] [-m mark] [-M pmtudisc_option] [-N node-info_option] [.w deadline] [-W timeout] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamps optioin] [hop…] destination

Opciones:

-a	Ping audible
-A	Ping adaptativo, se adapta al tiempo de ida y vuelta.
-b	Permite realizar ping a una dirección de broadcast.
-B	No permite ping para cambiar la dirección de origen de las pruebas.
-c count	Se para después de enviar (y recibir) paquetes ECHO_RESPONSE.

-i interval	Espera unos segundos entre el envío de cada paquete.
-i wait	Se esperan unos segundos entre el envío de cada paquete. Pordefecto se debe esperar durante un segundo entre cada paquete.
-l preload	Si no se específica precarga, ping envía todos los paquetes sin esperar respuesta.
-L	Suprime el bucle de retronó de los paquetes multicast, esta opción sólo se aplica si el destino del ping es una dirección multicast.
-m mark	Se especifica el valor de tiempo de vida usado para los paquetes que salen. El valor por defecto es 30 (por defecto también se usa en las conexiones TCP).
-n	Sólo salida numérica.
-O	Informe de la respuesta del eco ICMP antes de enviar el siguiente paquete.
-p pattern	Se puede especificar hasta 16 bytes "pad " para llenar el paquete que se envía. Esto es útil para diagnosticar problemas dependientes de datos en una red.
-q	No se muestra nada excepto el tiempo de inicio y cuando se termina.
-Q tos	Ajuste de calidad del servicio relacionado con los bits de datagramas ICMP.
-R	Un ping solo de registro de ruta. Incluye la opción de RECORD_ROUTE en la ECHO_REQUEST y muestra la ruta en los paquetes devueltos.
-s packetsize	Especifica el número de bytes de datos para ser enviados. Por defecto es 56, que traducido en bytes es 64 datos ICMP cuando combinado con 8 bytes de datos de header ICMP.
-t ttl	Ping TTL solo, ajusta el tiempo IP de vida del paquete.
-T	El ping funciona como traceroute, imprimiendo los paquetes de ruta a un host de red.
-U	Imprime la latencia completa del usuario.
-V	Muestra la versión y sale.
-w deadline	Especifica un tiempo de espera antes de que el ping termine.

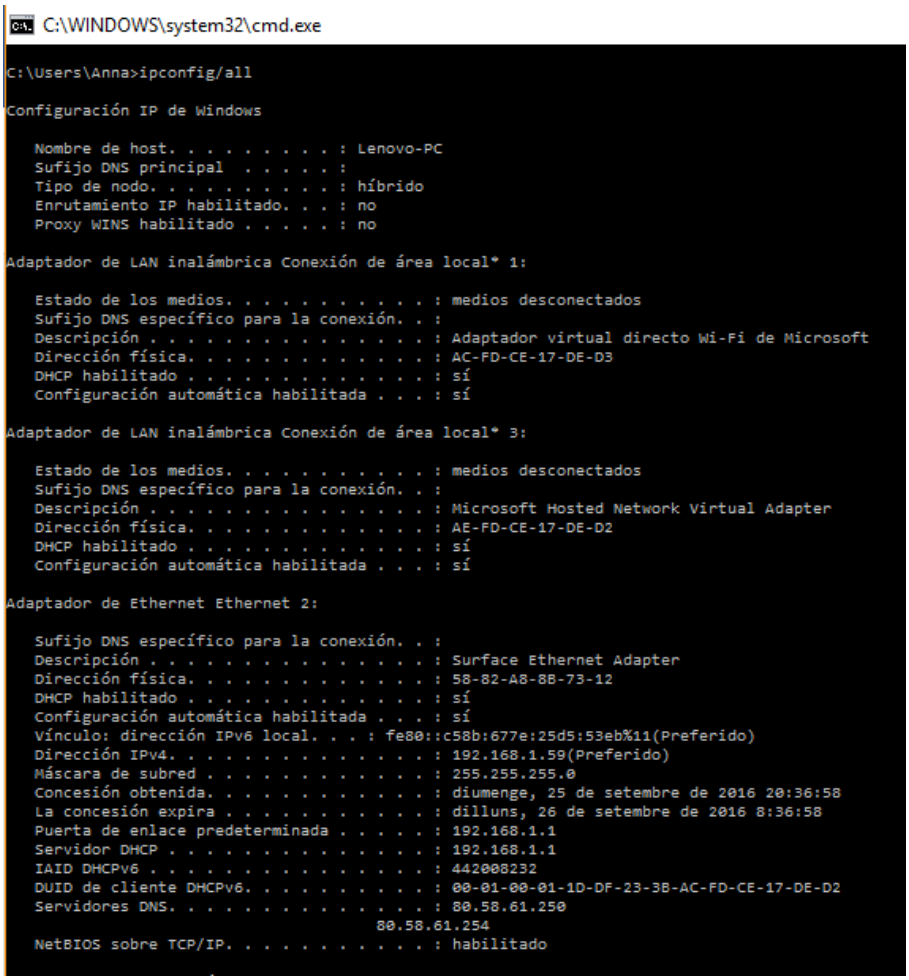
-W timeout	Pone el tiempo (en segundos) espera para r una respuesta a una prueba (por defecto es 3 segundos)

Tabla 8:2Comandos Linux para ping

8.7. IPconfig

Muestra la información relativa de los parámetros de configuración de IP actual. Se pueden agregar otros comandos para realizar otras funciones como recuperar y establecer parámetros de IP

Comando: ipconfig/all



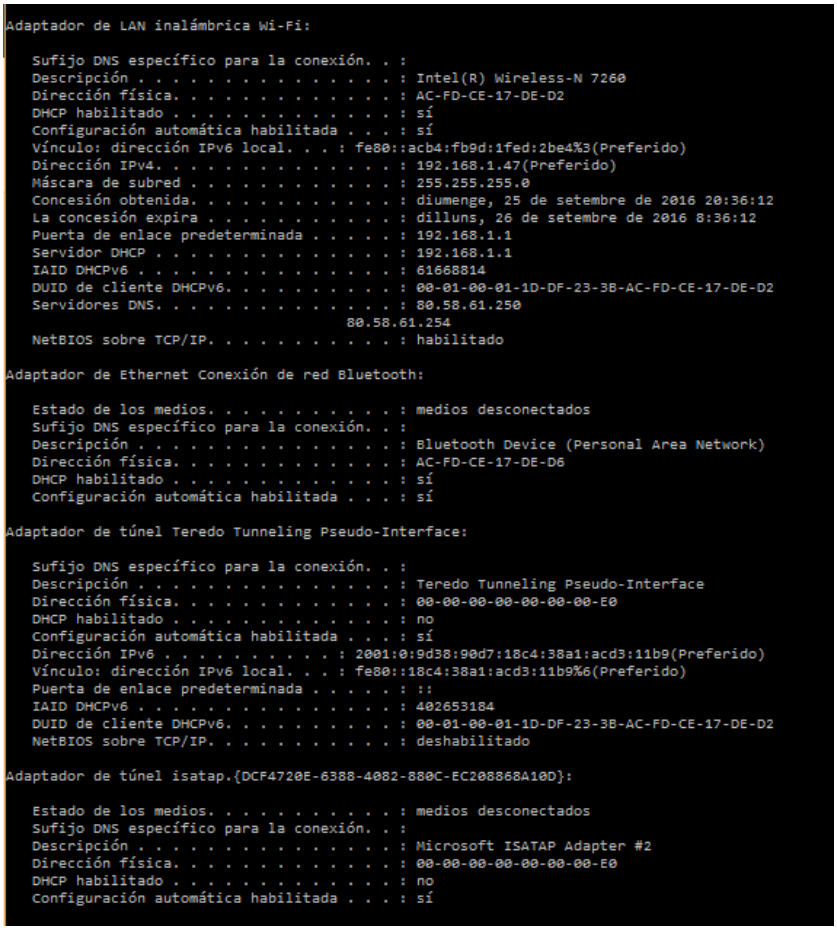


Figura 8:11: ipconfig/all en el usuario de prueba.

8.8. Netstat

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

-a	Muestra todas las conexiones y puertos de escucha. (Normalmente las conexiones del lado del servidor no se muestran).
-e	Muestra estadísticas Ethernet. Se puede combinar con la opción –s.
-n	Muestra direcciones y números de puerto en formato numérico.
-p proto	Muestra las conexiones del protocolo especificado por proto; proto puede ser tcp o udp. Utilizada con la opción –s para mostrar estadísticas por protocolo, proto puede ser tcp, udp, o ip.
-r	Muestra el contenido de la tabla de rutas
-s	Muestra estadísticas por protocolo. Por defecto, se muestran las estadísticas para TCP, UDP e IP; la opción –p puede ser utilizada para especificar un sub conjunto de los valores por defecto.

Tabla 8:3 Comandos netstat

8.9. Wireshark

Para acceder al análisis de llamadas VoIP, explicaremos los pasos a seguir.

1. Cargar en Wireshark el archivo .pcap que hemos extraído utilizando Sngrep y escogeremos una trama SIP.

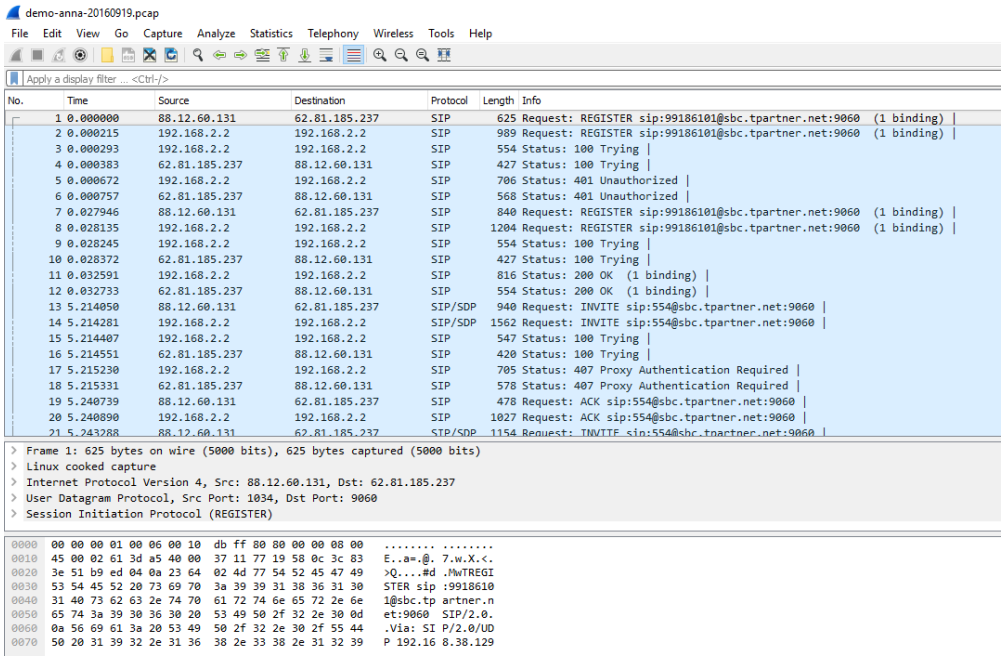


Figura 8:12 Archivo .pcap en Wireshark.

2. Para visualizar flujos de tráfico vamos al menú Statistics → Conversations

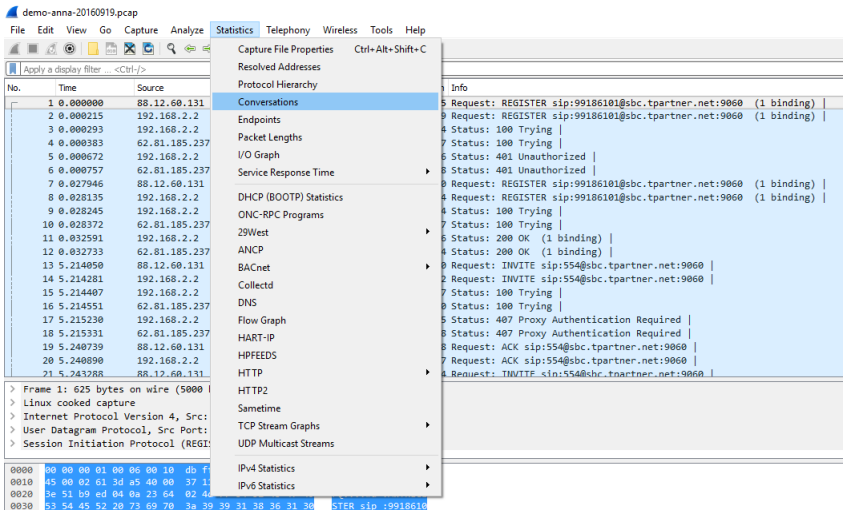


Figura 8:13 Como visualizar conversaciones

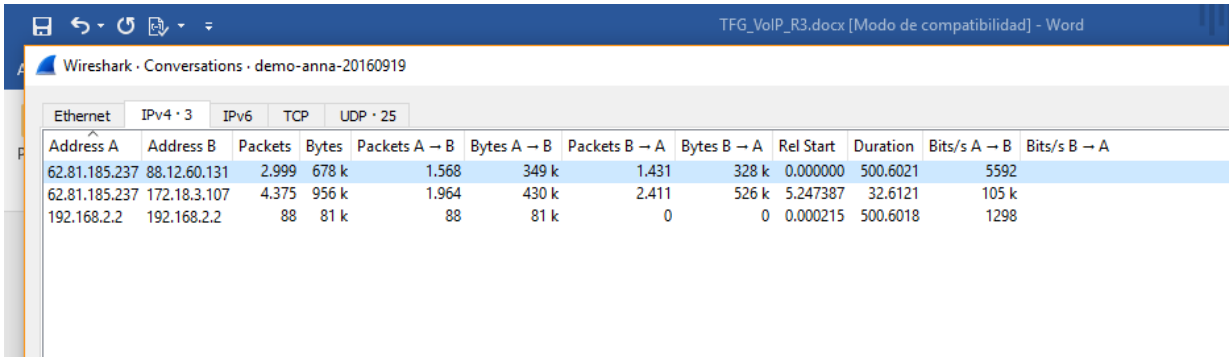


Figura 8:14 Diagrama de paquetes en las conversaciones.

3. Para examinar funcionalidades específicas para el análisis de VoIP, vamos al menú Telephony → VoIP Calls. Y cómo veremos podemos reproducir la conversación o bien ver un diagrama de flujo de la llamada.

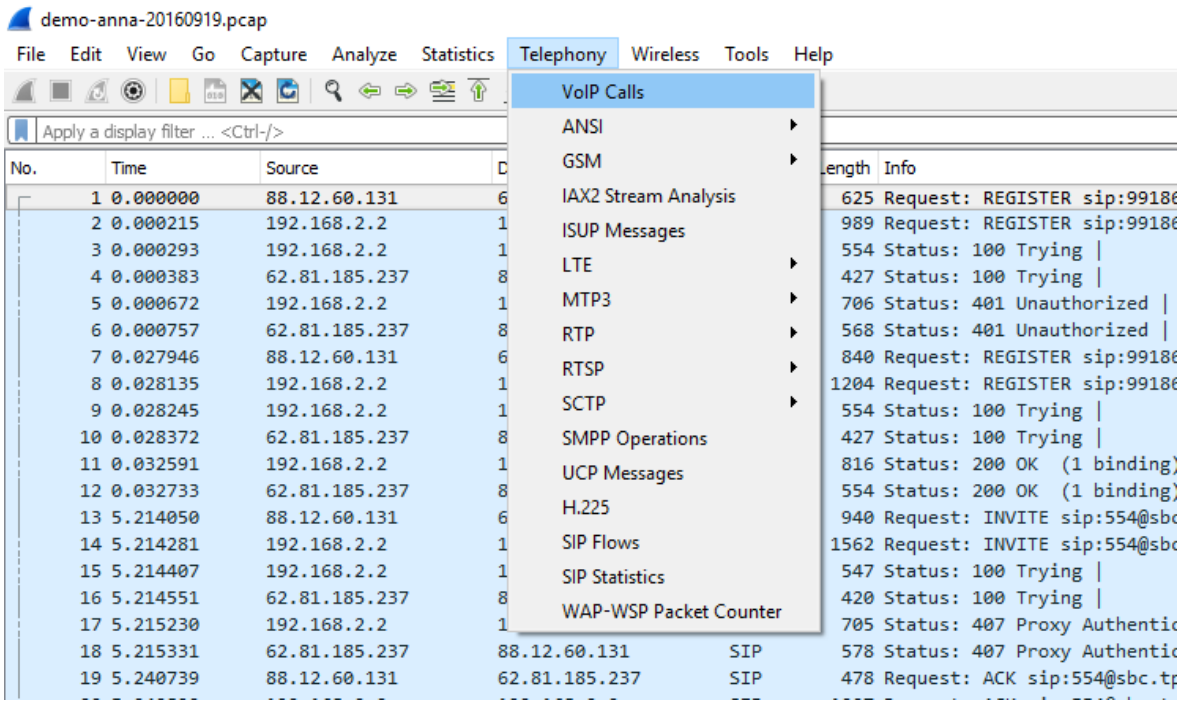


Figura 8:15 Pasos para visualizar las llamadas VoIP

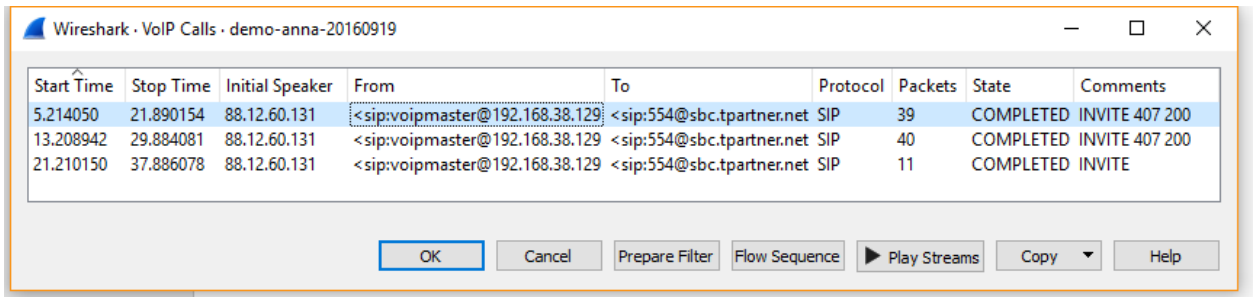


Figura 8:16 Visualización y opciones de reproducción de las conversaciones

4. Si elegimos reproducir la llamada nos aparecerá lo siguiente, donde podemos ver los fallos de audio, si ha habido silencio, ver el Jitter, RTP y otros parámetros.

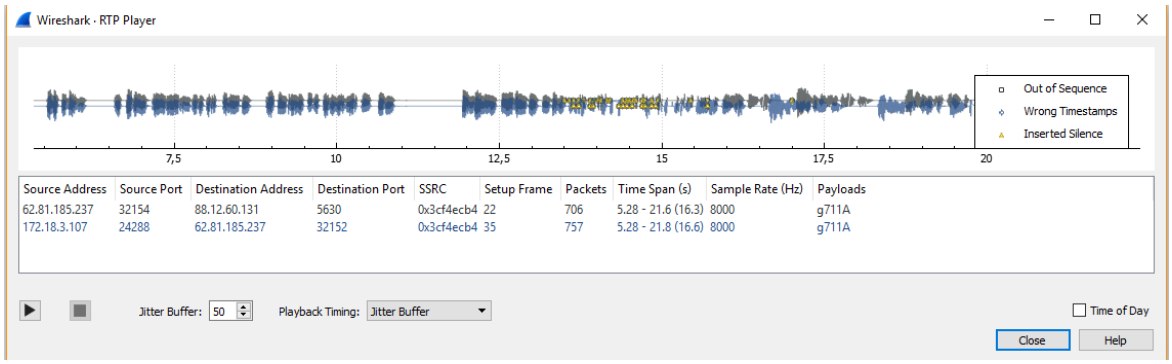


Figura 8:17 Cómo reproducir una conversación.

5. Si elegimos el flow sequence lo que visualizaremos será lo siguiente.

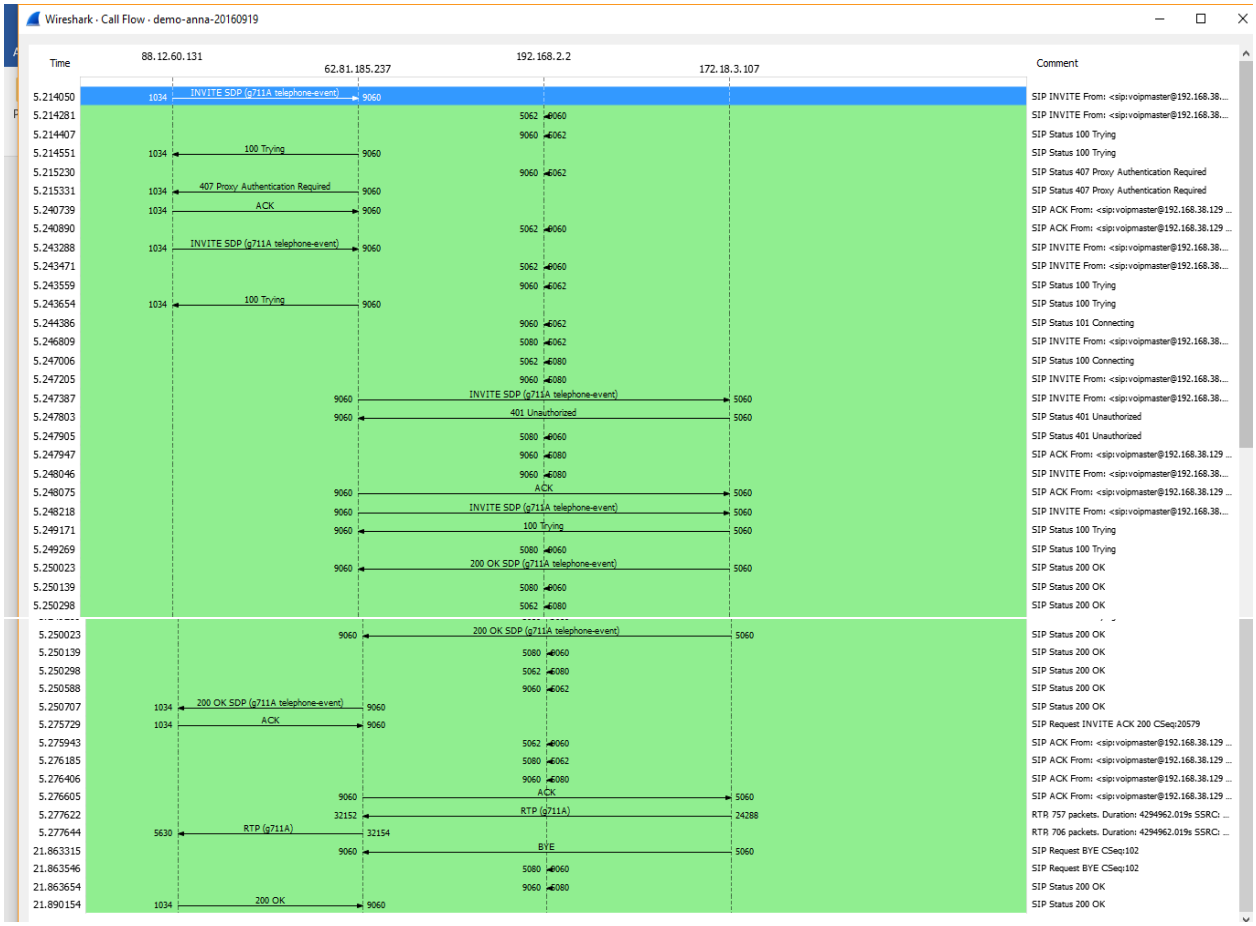


Figura 8:18 Diagrama de flujo de una conversación con wireshark.

8.10. Sngrep

sngrep [-hVcivNqrD] [-IO pcap_dump] [-d dev] [-l limit] [-k keyfile] [-LH capture_url] [<match expression>] [<bpf filter>]

-h –help	Ayuda
--version -V:	Información de la versión
-d --device	Utilizar este dispositivo de captura en lugar del que está por defecto
--input -I	Leer datos capturados desde un archivo pcap
-O --output	Escribir datos capturados a archivo pcap
-r --rtp	Captura de paquetes RTP
-l --limit	Establecer límite de captura a N cuadros de diálogo
-i --icase	Convertir mayúsculas a minúsculas y viceversa
-v --invert	Invertir
-N --no Interfaz	No mostrar la interfaz sngrep, simplemente capturar.
-q --quiet	No imprimir diálogos capturados si no utilizamos la interfaz
-D --dump-Config	Imprimir ajustes de configuración activos y de salida
-f --config	Leer configuración desde un archivo
-R --rotate	Girar llamadas cuando se ha alcanzado el límite de captura.
-H --eep-Send	url Homer sipcapture (UDP: X.X.X.X: XXXX)
-L---eep Escuchar	Escuchar paquetes encapsulados (UDP: X.X.X.X: XXXX)
-k --keyfile	RSA archivo clave privada para descifrar los paquetes capturados

Tabla 8:4 Comandos Sngrep

1. Iniciamos Sngrep en una consola de Linux → Sngrep

```
Linux sbc01 3.2.0-0.bpo.4-amd64 #1 SMP Debian 3.2.41-2+deb7u2~bpo60+1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 26 11:43:07 2016 from 90.red-80-39-72.staticip.rima-tde.net
 root@sbc01:~# sngrep
```

Figura 8:19 Como iniciar Sngrep.

2. En Tpartner tenemos que entrar en el servidor SBC.tparnter.net con su respectiva contraseña y ya podremos ver por pantalla todas los paquetes y diálogos que se están ejecutando en tiempo real en el servidor.

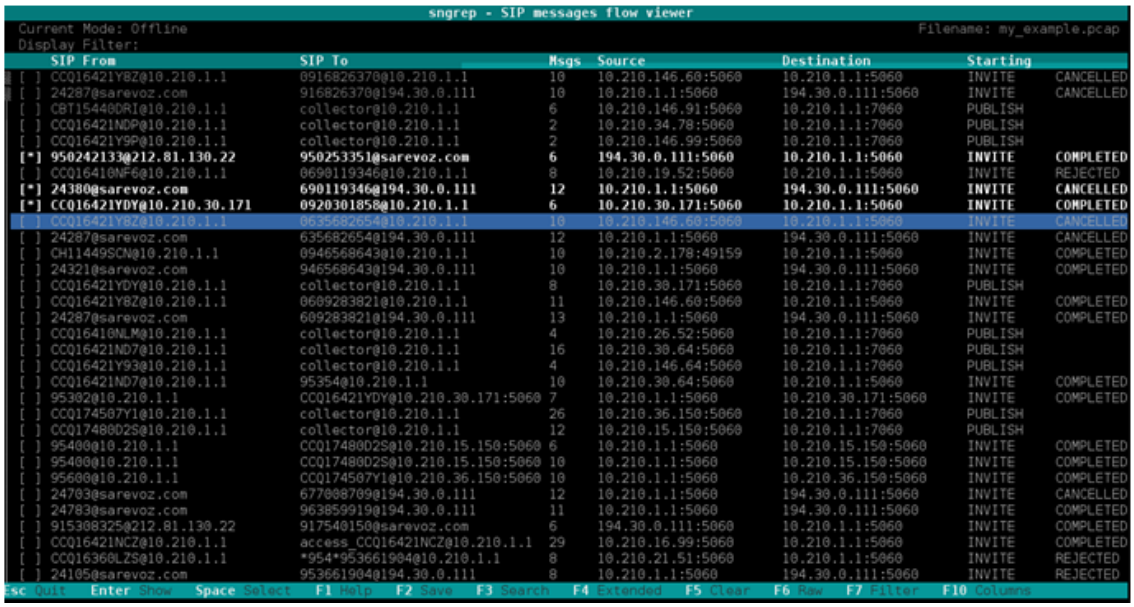


Figura 8:20 Consola y paquetes en Sngrep

3. Como sólo trabajamos con paquetes SIP, mediante un filtro indicamos que nos interesan únicamente estos paquetes. Se nos presenta una pantalla donde cada fila es un diálogo SIP las columnas nos muestran el origen, el destino…etc

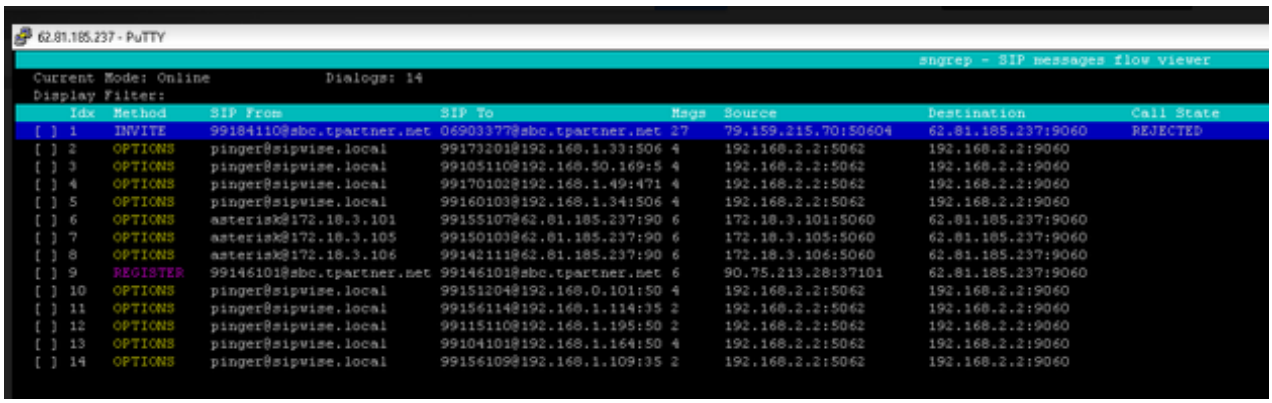


Figura 8:21 Filtro con los paquetes SIP

4. Las columnas son personalizables, pulsando F10 aparece la siguiente ventana con todos los campos que se pueden añadir, también podemos cambiar el orden de las columnas pulsando +/-.

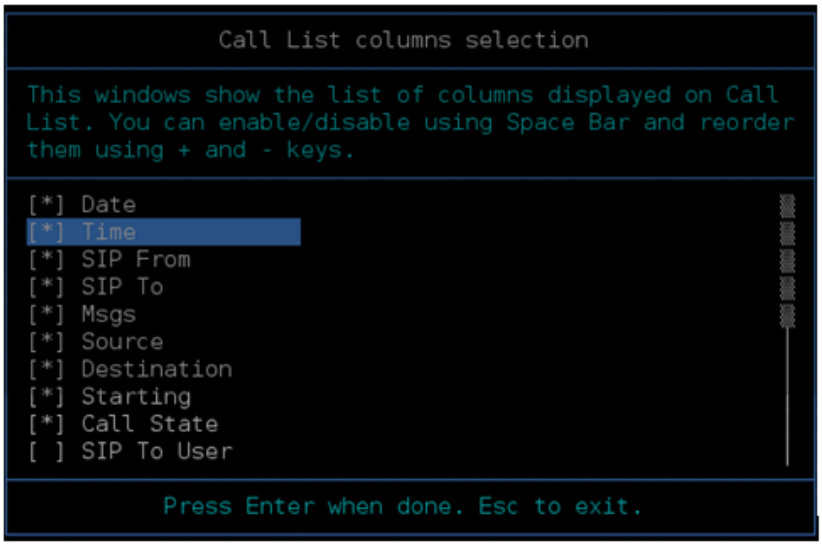


Figura 8:22 Selección de las columnas.

5. Accediendo a uno de los paquetes, nos aparecerá por pantalla un diagrama de flujo de la llamada realizada.

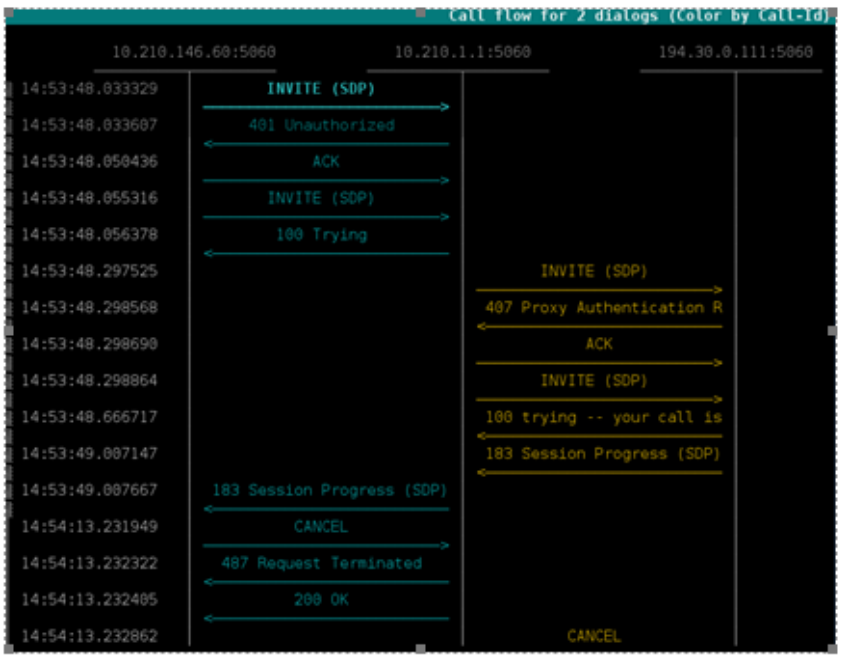


Figura 8:23 Diagrama de flujo con Sngrep

6. Si queremos guardarlo en modo texto, o archivo .pcap para poder visualizarlo en Wireshark una vez seleccionados los diálogos, pulsamos ‘r’ y después ‘s’, para guardarlo.

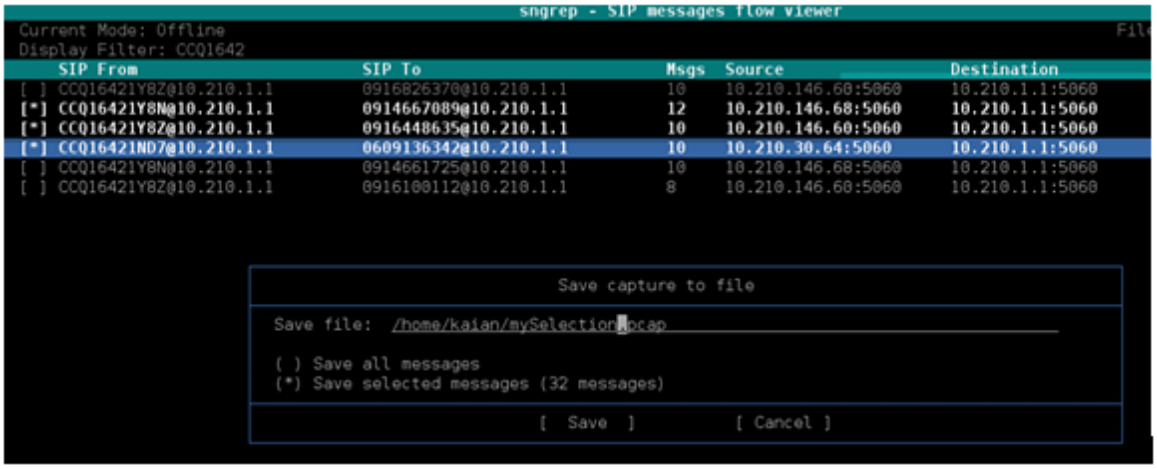


Figura 8:24 Cómo guardar un diálogo .pcap

Podemos hacer muchas otras cosas, comparar mensajes, ver registros, etc, pero no entraremos en más detalles en este trabajo, ya que no es objeto de éste explicar en profundidad el funcionamiento de sngrep.

8.11. VoipMaster

Como hemos dicho a lo largo del trabajo, VoIP master y sus respectivas pruebas han sido realizadas con el modo PBX, puesto que es el que nos interesa. A continuación, vemos la interfaz que tiene el programa, la explicaremos brevemente y veremos una serie de ejemplos de prueba y los informes que nos genera.

1. Cuando encendemos el ordenador con el USB bootable, el ordenador arranca con un sistema operativo Ubuntu. Por defecto, en el escritorio solo están dos iconos, el de VoIP master y el logo de la empresa en nuestro caso.

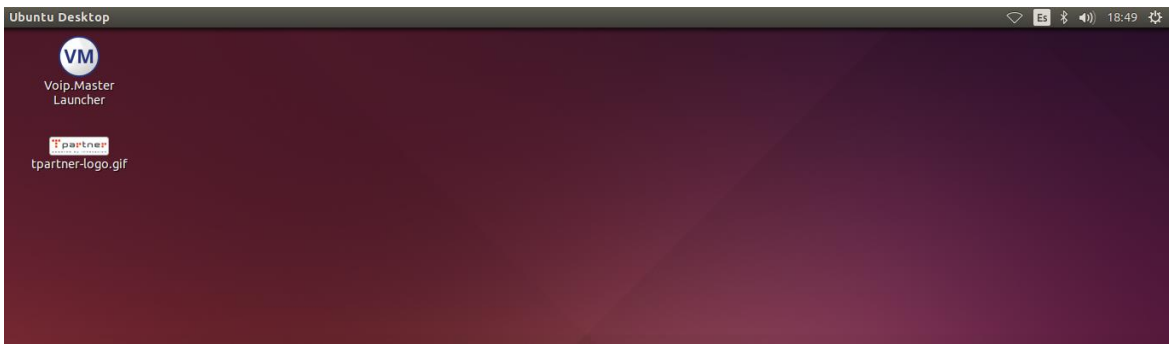


Figura 8:25Escritorio VoIP master.

2. Un requisito para que VoIP master funcione correctamente, es que tiene que estar conectado a la red con un cable ethernet. Una vez conectado y comprobamos que funciona correctamente Internet, iniciamos la aplicación haciendo doble clic en el icono.

Figura 8:26 VoIP master

3. Por defecto la aplicación tiene cargada una serie de perfiles para hacer pruebas, pero tenemos que configurar nosotros los perfiles de usuario que queremos, la conexión…etc. Pero previamente a configurar tenemos que escoger el modo en que queremos configurar los perfiles, y nosotros hemos escogido SIP_DHCP.

4. Una vez escogido el perfil nos aparecerá una ventana como la siguiente, y en tenemos que escoger configure, en el menú de la izquierda.

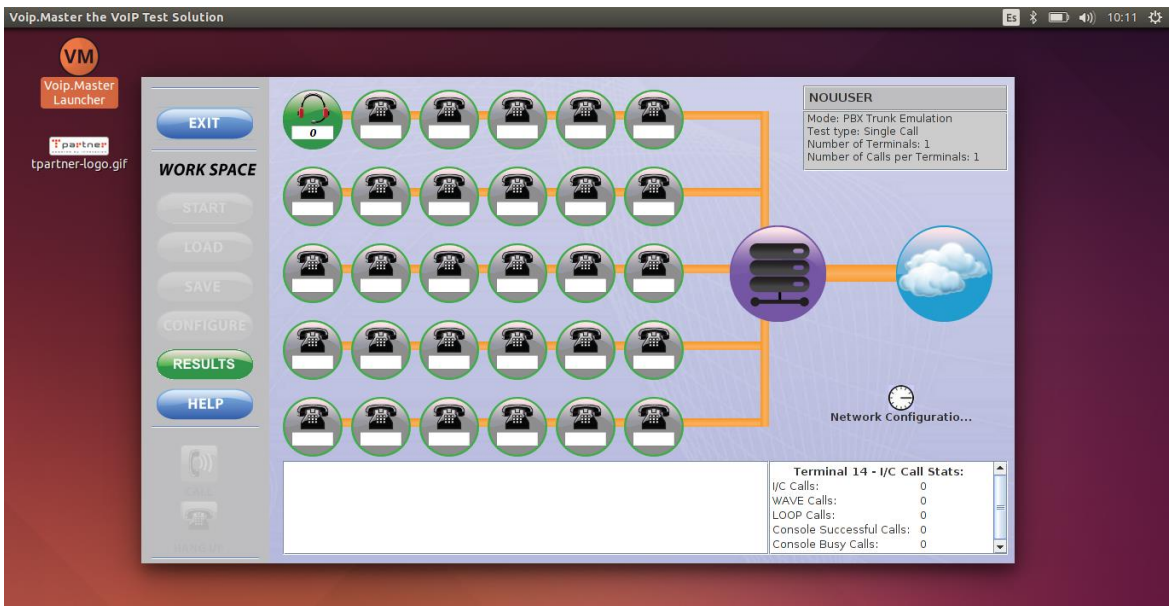


Figura 8:27 Perfil SIP_DHCP por defecto.

5. Opciones de configuración del test, en esta pestaña podemos escoger si queremos hacer una llamada simple, múltiples llamadas, cuantos terminales queremos que llamen, el retardo entre terminales y a qué números queremos que llamen.

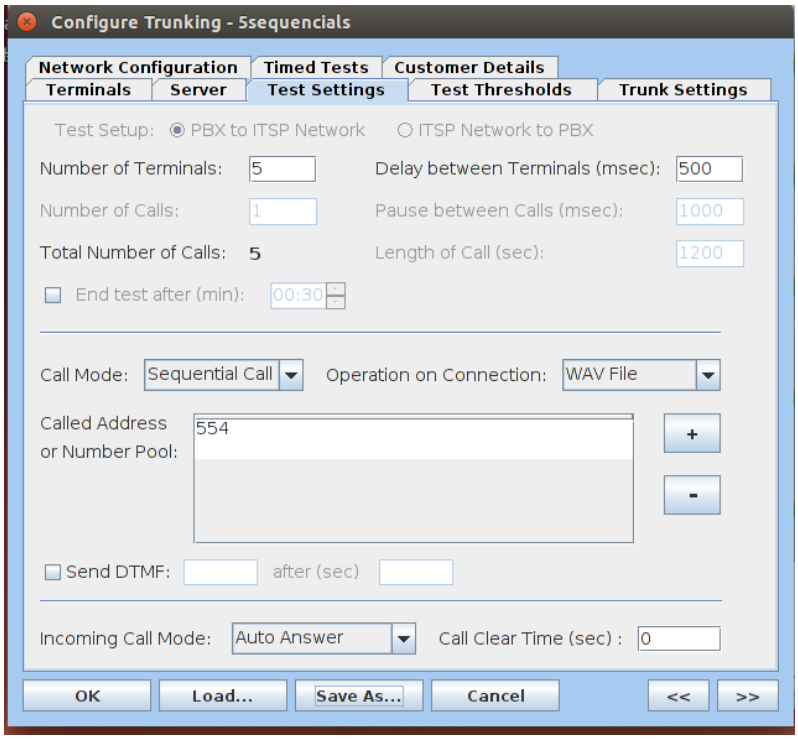


Figura 8:28 Test Settings

6. La pestaña de *test thresholds* sirve para configurar los parámetros de calidad a medir, que son los que necesitamos para la auditoría: Jitter, Delay, Pérdida de paquetes y la calidad MOS.

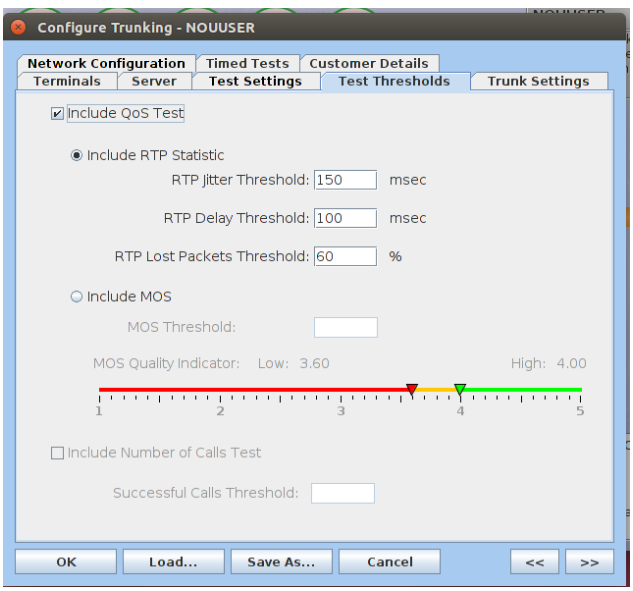


Figura 8:29 Test thresholds.

7. La pestaña Trunk Settings, sirve para configurar el servidor contra el que se harán las llamadas y pruebas.

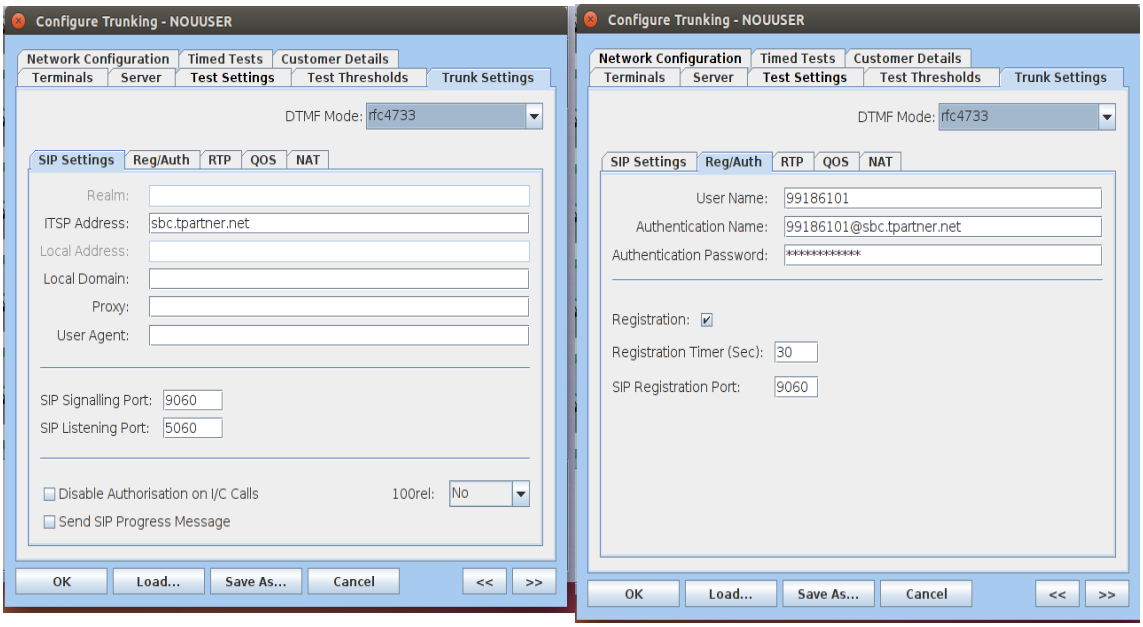


Figura 8:30 Trunk Settings

Una vez lo tenemos todo configurado realizaremos algunos ejemplos y sus resultados:

Ejemplo 1: Una llamada Simple.

Cuando tenemos un perfil configurado, como es nuestro caso, que podemos hacer pruebas con el servidor de Tpartner, configuramos un solo terminal para que realice una llamada con tráfico de voz, lo que sucederá es que el terminal se registra en el SBC de Tpartner, y realiza una llamada a una sala de videoconferencias, una vez finalizada la llamada, colgamos y si el test se ha realizado correctamente aparecerá un mensaje de PASS en verde, por el contrario si hay algún fallo aparecerá el mensaje FAIL en rojo.

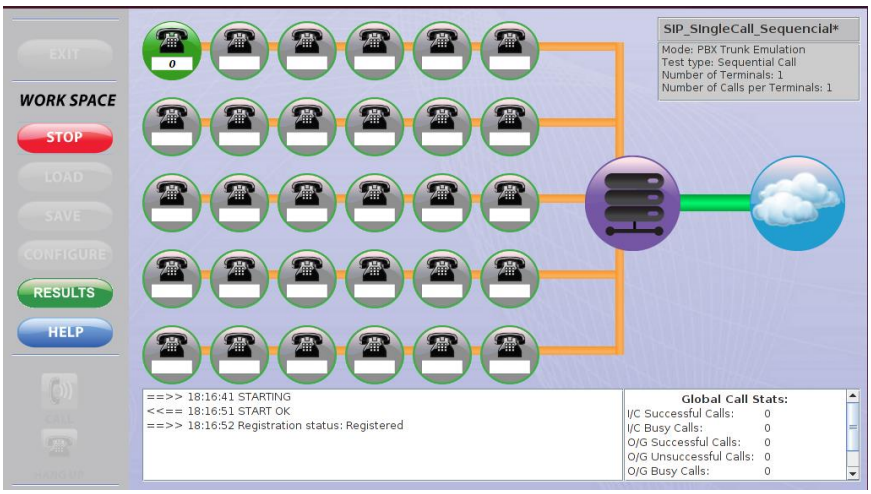


Figura 8:31 Registro de terminal para realizar la llamada

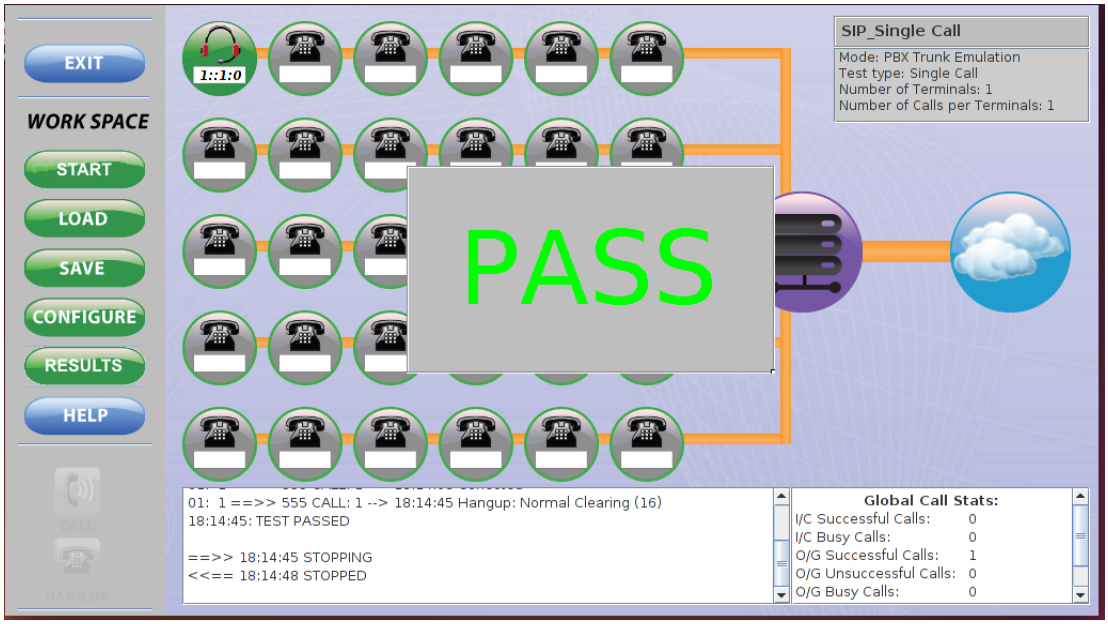


Figura 8:32 resultado correcto.

Ejemplo 2: Múltiples terminales realizando cada uno una llamada.

Lo mismo ocurre para múltiples usuarios que realizan una llamada cada uno, pero la inician cuando el anterior ha colgado.

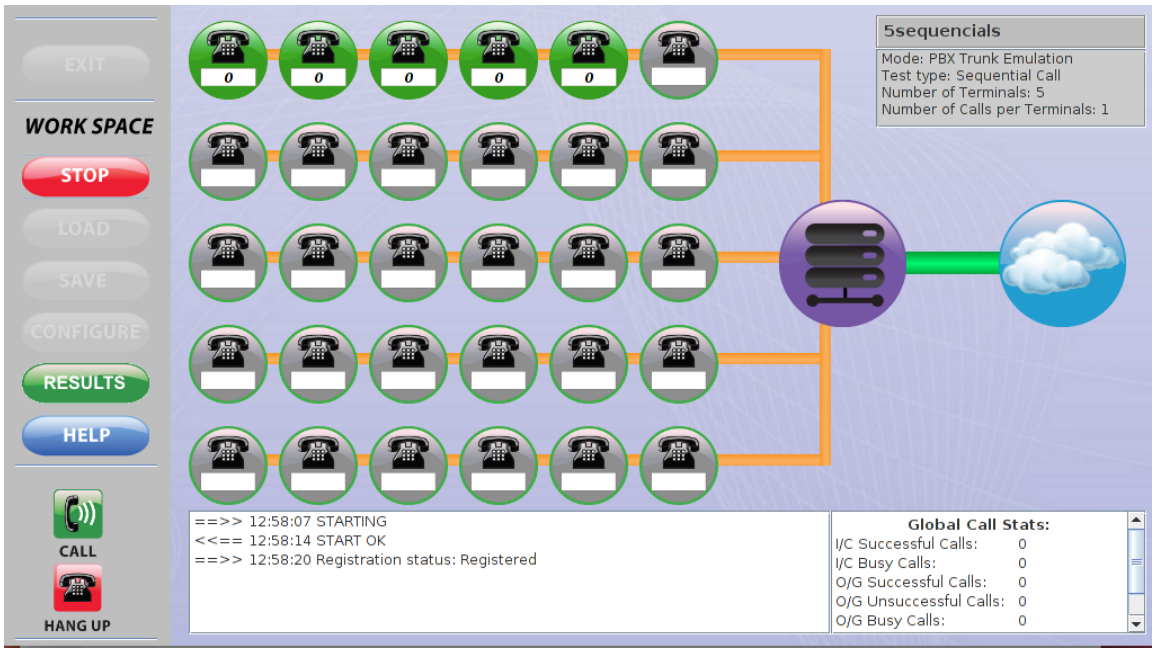


Figura 8:33 5 usuarios registrados

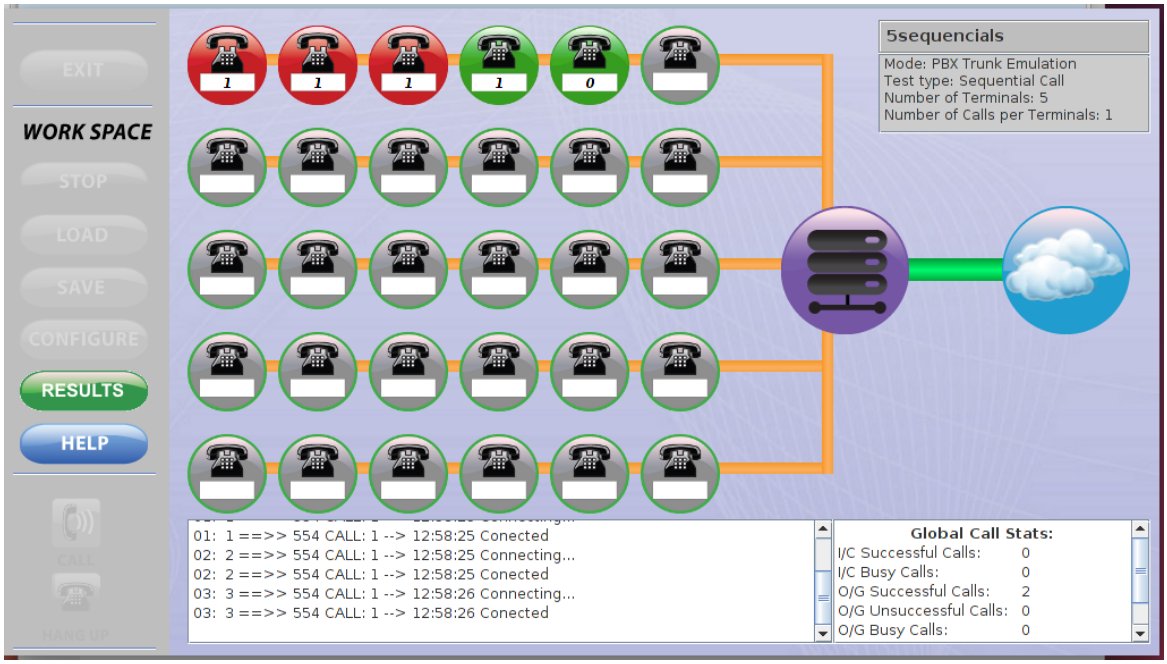


Figura 8:34 Usuarios llamando.

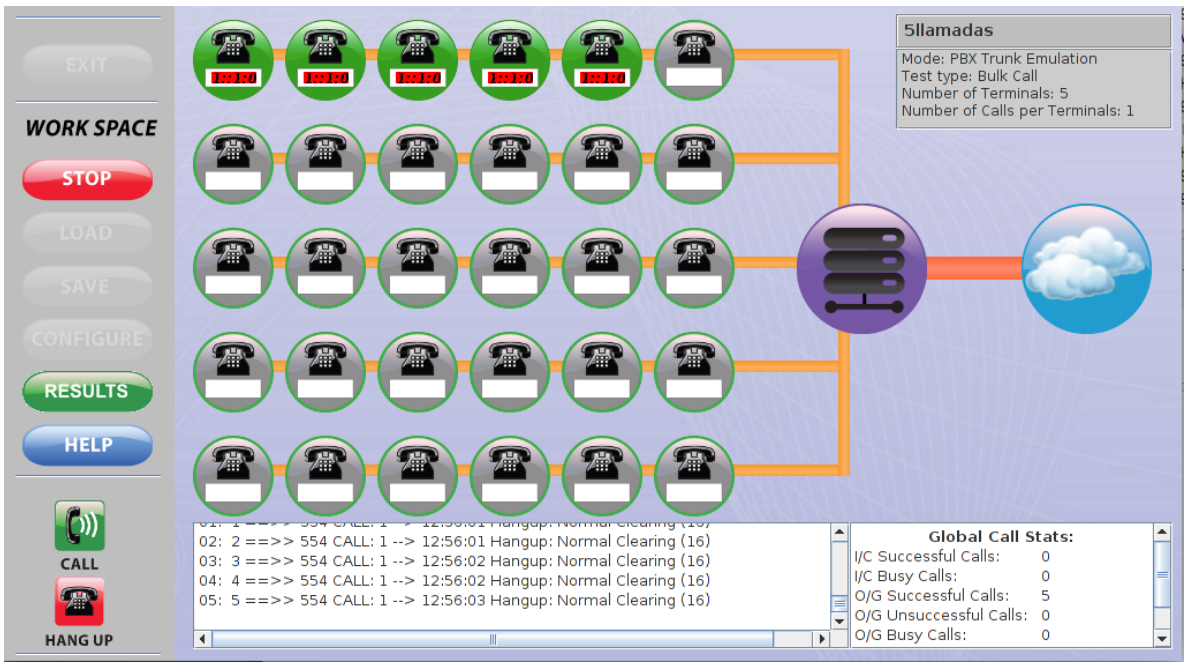


Figura 8:35 Prueba finalizada.

A continuación, adjuntaremos los informes generados tal y como los extrae VoIP master. Otras pruebas realizadas y no adjuntas han sido:

- Generar una llamada durante varias horas para comprobar la duración y calidad de la llamada.
- Generar una llamada y mientras se inyecta ruido para ver cómo ve afecta a la llamada.

Ejemplo 3: Informe del informe completo generado:

En este ejemplo hecho a partir de una configuración PBX, 1 llamada al 554, que es un número que tenemos configurado en nuestra centralita virtual como una sala de conferencias, hemos realizado la llamada.

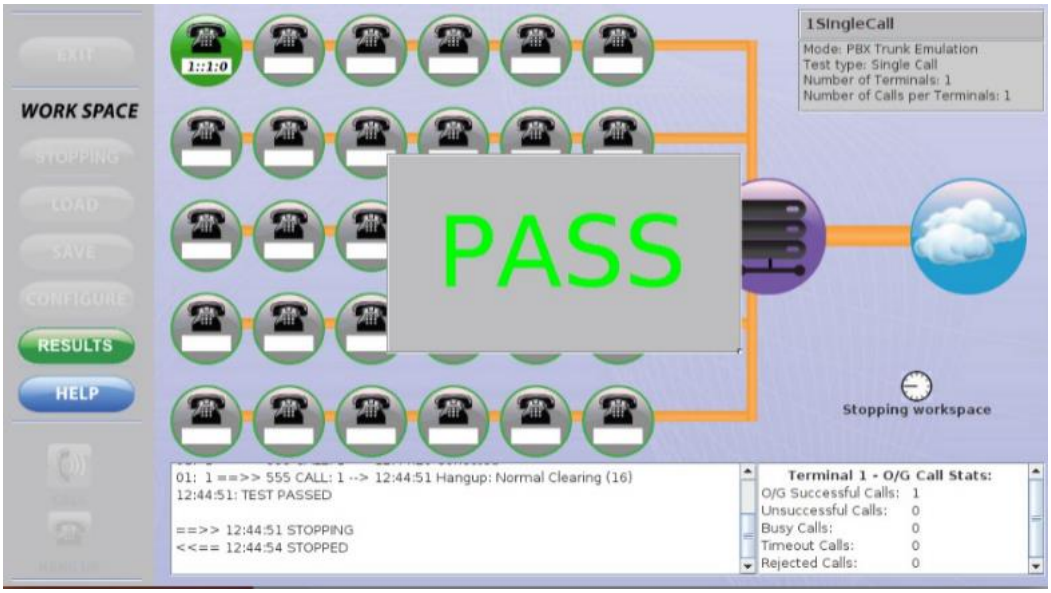


Figura 8:36 Realización de una llamada con éxito.

Profile name:	1SIngleCall.cvs
Test type:	Single Call
Operation on connection:	WAV File
Number of active terminals:	1
Number of calls per terminal:	1

Terminal	Local Number		Remote Number	Call	Time	Call Status
==>> 12:42:59 STARTING						
<<== 12:43:06 START OK						
==>> 12:43:08 Registration status: Registered						
01:	1	==>>	555	1	12:44:20	Connecting...
01:	1	==>>	555	1	12:44:20	Conected
01:	1	==>>	555	1	12:44:51	Hangup: Normal Clearing (16)
12:44:51: TEST PASSED						
==>> 12:44:51 STOPPING						
<<== 12:44:54 STOPPED						

Figura 8:37 El diagrama de flujo que genera VoIP Master

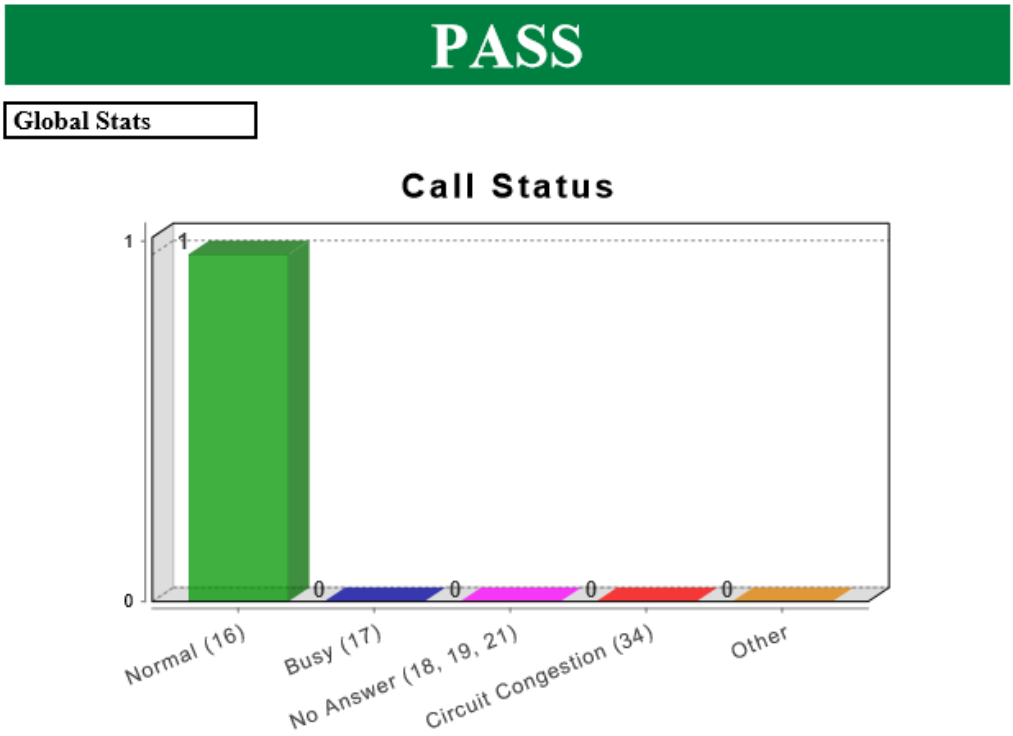
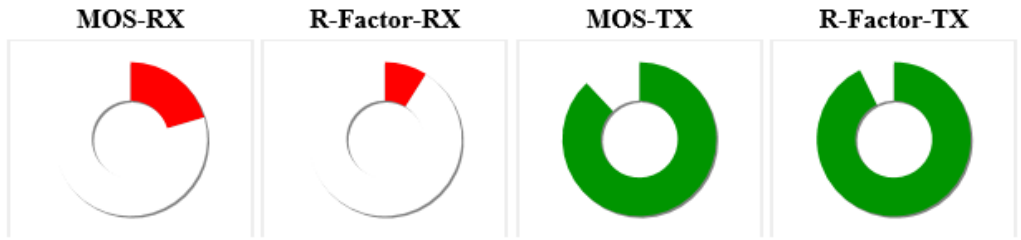


Figura 8:38 Si ha pasado o no la prueba.



RX	IA Jitter (ms)	RTT Delay (ms)	Loss (%)	Max Jitter (ms)	Min Jitter (ms)	Max RTT (ms)	Min RTT (ms)
	0.32	23.20	7.49	1.39	0.02	23.73	22.55

TX	IA Jitter (ms)	RTT Delay (ms)	Loss (%)	Max Jitter (ms)	Min Jitter (ms)	Max RTT (ms)	Min RTT (ms)
	0.68	23.20	0.00	1.20	0.40	23.73	22.55

Figura 8:39 Resumen de parámetros QoS del emisor y receptor

Terminal Stats - RX									
Terminal	**IA Jitter (ms)**	**RTT Delay (ms)**	**Loss (%)**	**Max Jitter (ms)**	**Min Jitter (ms)**	**Max RTT Delay (ms)**	**Min RTT Delay (ms)**	**MOS**	**R_Factor**
1	0.32	23.20	7.49	1.39	0.02	23.73	22.55	1.02	8.98

Terminal Stats - TX									
Terminal	**IA Jitter (ms)**	**RTT Delay (ms)**	**Loss (%)**	**Max Jitter (ms)**	**Min Jitter (ms)**	**Max RTT Delay (ms)**	**Min RTT Delay (ms)**	**MOS**	**R_Factor**
1	0.68	23.20	0.00	1.20	0.40	23.73	22.55	4.40	92.79

Figura 8:40 Resumen de parámetro totales, incluyendo el MOS.

Acrónimos

- **ADC**: Analog to Digital Converter (Convertidor de análogo a digital).
- **ATA**: Adaptador de Teléfono Analógico.
- **DAC**: Digital to Analog Converter (Convertidor de digital a análogo).
- **DNS:** Domain Name System (Sistema de Nombres de Dominio)
- **E.164:** Recomendación de la ITU-T para la numeración telefónica internacional, especialmente para ISDN, BISDN y SMDS.
- **H.323:** Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real en redes de área local, LAN, e Internet.
- **HSS:** Home Suscriber Server
- **HLR:** Home Location Register
- **IN:** Intelligent Network (Red Inteligente)
- **IP:** Internet Protocol (Protocolo Internet)
- **IPBX:** Internet Protocol Private Branch Exchange (Centralita Privada basada en IP)
- **ISDN:** Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI)
- **ITSP:** Internet Telephony Service Provider (Proveedor de Servicios de Telefonía Internet, PSTI)
- **ITU-T:** International Telecommunications Union - Telecommunications (Unión Internacional de Telecomunicaciones - Telecomunicaciones)
- **LAN:** Local Access Network
- **LDP:** Label Distribution Protocol (Protocolo de Distribución de Etiquetas)
- **LSR:** Label Switching Router (Encaminador de Conmutación de Etiquetas)
- **MEGACO:** Media Gateway Control (Control de Pasarela de Medios)
- **MGC:** Media Gateway Controller (Controlador de Pasarela de Medios)
- **MGCP:** Media Gateway Control Protocol (Protocolo de Control de Pasarela de Medios)
- **MOS:** Mean Opinion Score (Nota Media de Resultado de Opinión)
- **NAT:** Network Address Translation (Traductor de direcciones de red)
- **PBX:** Private Branch Exchange (Centralita Telefónica Privada)
- **PCM:** Pulse Code Modulation (Modulación Pulso Código)
- **PoP:** Point of Presence (Punto de Presencia)
- **PSTN:** Public Switched Telephone Network (Red de Telefonía Conmutada Pública)
- **QoS:** Quality of Service (Calidad de Servicio)
- **RTCP:** Real Time Control Protocol (Protocolo de Control de Tiempo Real)
- **RTP:** Real Time Protocol (Protocolo de Tiempo Real)
- **SDP:** Session Description Protocol (Protocolo de Descripción de Sesión)
- **SIP:** Session Initiation Protocol (Protocolo de Inicio de Sesión)
- **SLA:** Service Level Agreement (Acuerdo de Nivel de Servicio)
- **TCP:** Transmission Control Protocol (Protocolo de Control de Transmisión)
- **TDM:** Time Division Multiplexing (Multiplexado por División de Tiempo)
- **UDP:** User Datagram Protocol (Protocolo de Datagramas de Usuario)
- **UMTS:** Universal Mobile Telephone System (Sistema Universal de Telecomunicaciones Móviles)
- **VLAN:** Virtual Local Area Network (Red de Área Local Virtual)
- **VoIP:** Voice over Internet Protocol (Voz sobre Protocolo de Internet)
- **VPN:** Virtual Private Network (Red Privada Virtual)